



8e6® R3000 | Enterprise Filter

USER GUIDE

for Authentication



Model: R3000

Release 1.10.20 / Version No.: 1.01

R3000 ENTERPRISE FILTER AUTHENTICATION USER GUIDE

© 2006 8e6 Technologies
All rights reserved.
828 W. Taft Ave., Orange, CA 92865, USA

Version 1.01, published December 2006
To be used with R3000 User Guide version 1.01 for software
release 1.10.20

Printed in the United States of America

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from 8e6 Technologies.

Every effort has been made to ensure the accuracy of this document. However, 8e6 Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. 8e6 Technologies shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

The latest version of this document can be obtained from
http://www.8e6.com/docs/r3000_auth_ug.pdf.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# R3.10_AUG_v1.01-0612

CONTENTS

CHAPTER 1: INTRODUCTION	1
About this User Guide	1
How to Use this User Guide	2
Conventions	2
Terminology	3
Filtering Elements	8
Group Types	8
Global Group	8
IP Groups	9
NT Domain Groups	10
LDAP Domain Groups	11
Filtering Profile Types	12
Static Filtering Profiles	13
Master IP Group Filtering Profile	13
IP Sub-Group Filtering Profile	13
Individual IP Member Filtering Profile	13
Active Filtering Profiles	14
Global Filtering Profile	14
NT/LDAP Group Filtering Profile	14
NT/LDAP Member Filtering Profile	14
Override Account Profile	15
Time Profile	15
Lock Profile	15
Filtering Profile Components	16
Library Categories	17
8e6 Supplied Categories	17
Custom Categories	17
Service Ports	18
Rules	18
Minimum Filtering Level	18
Filter Settings	19
Filtering Rules	20
Authentication Operations	23
R3000 Authentication Protocols	23

R3000 Authentication Tiers	23
Tier 1: Single Sign-On Authentication	25
Net use based authentication process	25
Re-authentication process	26
Authentication methods	27
SMB protocol.....	27
SMB Signing.....	27
LDAP protocol	28
Name resolution methods	29
Authentication setup procedures	30
Server setup types	30
Tier 1: Net use based authentication.....	30
Tier 2 and Tier 3: Web-based authentication.....	30
Configuring the authentication server	31
Login scripts	32
Enter net use syntax in the login script.....	32
View login script on the server console	33
Block page authentication login scripts.....	34
LDAP server setup rules	35
Tier 2: Time-based, Web Authentication	36
Tier 2 implementation in an environment	37
Tier 2 Script	38
Tier 1 and Tier 2 Script	39
Tier 3: Session-based, Web Authentication	41
8e6 Authenticator	42
Environment requirements	42
Minimum system requirements	42
Recommended system requirements	43
Workstation requirements	43
Work flow in a Windows environment	44
8e6 Authenticator configuration priority	45
8e6 Authenticator configuration syntax	46
Sample command line parameters	46
Table of parameters	47
Novell eDirectory Agent	50
Environment requirements	50
Novell eDirectory servers	50
Client workstations	51
Novell clients	51
Novell eDirectory setup	51
R3000 setup and event logs	52

Authentication Solution Compatibility	53
Configuring the R3000 for Authentication	54
Configuration procedures	54
System section	54
Group section	57
CHAPTER 2: NETWORK SETUP	58
Environment Requirements	58
Workstation Requirements	58
Administrator	58
End User	58
Network Requirements	59
Set up the Network for Authentication	60
Specify the operation mode	60
Specify the subnet mask, IP address(es)	62
Invisible mode	63
Router or firewall mode	63
Enable authentication, specify criteria	64
Net use based authentication	66
Web-based authentication	67
Enter network settings for authentication	70
Create an SSL certificate	72
Create, Download a Self-Signed Certificate	73
Create, Upload a Third Party Certificate	74
Create a Third Party Certificate	74
Upload a Third Party Certificate	76
Download a Third Party Certificate	77
View log results	78
Specify block page settings	81
Block Page Authentication	82
Block page	83
User/Machine frame	84
Standard Links	84
Optional Links	85
Options page	86
Option 1	87
Option 2	88
Option 3	89
Common Customization	90

Enable, Disable Features	91
Authentication Form Customization	93
Preview Sample Authentication Request Form	95
Block Page Customization	97
Preview Sample Block Page	99
CHAPTER 3: NT AUTHENTICATION SETUP	101
Join the NT Domain	101
Create an NT Domain	103
Add an NT domain	103
Refresh the NT branch	104
View or modify NT domain details	105
Domain Settings	105
Default Rule	107
Delete an NT domain	108
Set up NT Domain Groups, Members	109
Add NT groups, members to the tree	109
Specify a group's filtering profile priority	111
Manually add a user's name to the tree	113
Manually add a group's name to the tree	114
Upload a file of filtering profiles to the tree	115
Create and Maintain NT Profiles	118
Add an NT group, member to the tree list	118
Add or maintain an entity's profile	120
Category Profile	121
Redirect URL	122
Filter Options	123
Remove an entity's profile from the tree	124
CHAPTER 4: LDAP AUTHENTICATION SETUP	125
Create an LDAP Domain	125
Add the LDAP domain	125
Refresh the LDAP branch	126
View, modify, enter LDAP domain details	126
LDAP Server Type	127
Group Objects	128

User Objects	130
Address Info	131
Account Info	134
SSL Settings	135
Alias List	137
Default Rule	139
Default Rule for Novell eDirectory	141
Configure a backup server.....	141
Modify a backup server's configuration	145
Delete a backup server's configuration.....	145
Delete a domain	145
Set up LDAP Domain Groups, Members	146
Add LDAP groups, users to the tree	146
Perform a basic search	147
Options for search results	147
Apply a filtering rule to a profile	148
Delete a rule	149
Specify a group's filtering profile priority	149
Manually add a user's name to the tree	150
Manually add a group's name to the tree	151
Upload a file of filtering profiles to the tree	152
Create, Maintain LDAP Profiles	155
Add an LDAP group, member to the tree	155
Add or maintain an entity's profile	157
Category Profile	158
Redirect URL	159
Filter Options	160
Remove an entity's profile from the tree	161
CHAPTER 5: AUTHENTICATION DEPLOYMENT	162
Test Authentication Settings	162
Test Web-based authentication settings	164
Step 1: Create an IP Group, "test"	164
Step 2: Create a Sub-Group, "workstation"	165
Step 3: Set up "test" with a 32-bit net mask	166
Step 4: Give "workstation" a 32-bit net mask	167
Step 5: Block everything for the Sub-Group	168
Step 6: Use Authentication Request Page for redirect URL ...	169

Step 7: Disable filter options	170
Step 8: Attempt to access Web content	171
Test net use based authentication settings	173
Activate Authentication on the Network	174
Activate Web-based authentication for an IP Group	175
Step 1: Create a new IP Group, “webauth”	175
Step 2: Set “webauth” to cover users in range	176
Step 3: Create an IP Sub-Group	177
Step 4: Block everything for the Sub-Group	179
Step 5: Use Authentication Request Page for redirect URL ...	180
Step 6: Disable filter options	181
Step 7: Set Global Group to filter unknown traffic	182
Activate Web-based authentication for the Global Group	187
Step 1: Exclude filtering critical equipment	187
Step 1A: Block Web access, logging via Range to Detect	188
Range to Detect Settings	188
Range to Detect Setup Wizard	190
Step 1B: Block Web access via IP Sub-Group profile	196
Step 2: Modify the Global Group Profile	199
Activate NT authentication	203
Step 1: Modify the 3-try login script	203
Step 2: Modify the Global Group Profile	204
 CHAPTER 6: TECHNICAL SUPPORT	 206
 Hours	 206
 Contact Information	 206
Domestic (United States)	206
International	206
E-Mail	206
Office Locations and Phone Numbers	207
8e6 Corporate Headquarters (USA)	207
8e6 Taiwan	207
8e6 China	207
 Support Procedures	 208
 APPENDIX A	 209

User/Group File Format and Rules	209
Username Formats	209
Rule Criteria	210
File Format: Rules and Examples	212
NT User List Format and Rules	213
NT Group List Format and Rules	214
LDAP User List Format and Rules	215
LDAP Group List Format and Rules	217
 APPENDIX B	 218
Ports for Authentication System Access	218
 APPENDIX C	 219
LDAP Server Customizations	219
OpenLDAP Server Scenario	219
Not all users returned in User/Group Browser	219
 APPENDIX D	 220
Disable SMB Signing Requirements	220
SMB Signing Compatibility	220
Disable SMB Signing Requirements in Windows 2003	221
 APPENDIX E	 226
Obtain or Export an SSL Certificate	226
Export an Active Directory SSL Certificate	226
Verify certificate authority has been installed	226
Locate Certificates folder	227
Export the master certificate for the domain	230
Export a Novell SSL Certificate	234
Obtain a Sun ONE SSL Certificate	235
 APPENDIX F	 236
Override Pop-up Blockers	236
Yahoo! Toolbar Pop-up Blocker	237

If pop-up blocking is enabled	237
Add override account to the white list	237
Google Toolbar Pop-up Blocker	239
If pop-up blocking is enabled	239
Add override account to the white list	239
AdwareSafe Pop-up Blocker	240
If pop-up blocking is enabled	240
Temporarily disable pop-up blocking	240
Mozilla Firefox Pop-up Blocker	241
Add override account to the white list	241
Windows XP SP2 Pop-up Blocker	242
Set up pop-up blocking	242
Use the Internet Options dialog box.....	242
Use the IE toolbar	243
Temporarily disable pop-up blocking	243
Add override account to the white list	244
Use the IE toolbar	244
Use the Information Bar	245
Set up the Information Bar.....	245
Access your override account.....	245
APPENDIX G	247
Glossary	247
INDEX	255

CHAPTER 1: INTRODUCTION

The R3000 Authentication User Guide contains information about setting up authentication on the network.

About this User Guide

This user guide addresses the network administrator designated to configure and manage the R3000 server on the network.

Chapter 1 provides information on how to use this user guide, and also includes an overview of filtering components and authentication operations.

Chapters 2, 3, and 4 describe the R3000 Administrator console entries that must be made in order to prepare the network for using authentication for NT and/or LDAP domains.



NOTE: Refer to the *R3000 Quick Start Guide* for information on installing the unit on the network. This document also provides information on how to access the R3000 console to perform the initial installation setup defined in Chapter 2: Network Setup.

After all settings have been made, authentication is ready to be used on the network. Chapter 5 outlines the step you need to take to test and to activate your settings before deploying authentication on the network.

Chapter 6 provides support information. Appendices at the end of this user guide feature instructions on filtering profile file components and setup; a chart of ports used for authentication system access; notes on customizations to make on specified LDAP servers; steps to modify the SMB protocol to disable SMB Signing requirements; information on how to obtain or export an SSL certificate and upload it to the R3000; tips on how to override pop-up windows with pop-up

blocker software installed; a glossary on authentication terms, and an index.

How to Use this User Guide

Conventions

The following icons are used throughout this user guide:



NOTE: The “note” icon is followed by italicized text providing additional information about the current subject.



TIP: The “tip” icon is followed by italicized text giving you hints on how to execute a task more efficiently.



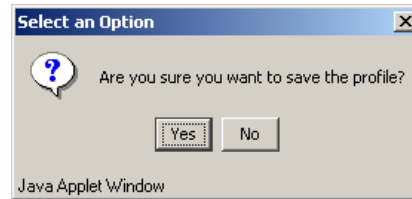
WARNING: The “warning” icon is followed by italicized text cautioning you about making entries in the application, executing certain processes or procedures, or the outcome of specified actions.

Terminology

The following terms are used throughout this user guide. Sample images (not to scale) are included for each item.

- **alert box** - a message box that opens in response to an entry you made in a dialog box, window, or screen. This box often contains a button (usually labeled “OK”) for you to click in order to confirm or execute a command.
- **button** - an object in a dialog box, window, or screen that can be clicked with your mouse to execute a command.
- **checkbox** - a small square in a dialog box, window, or screen used for indicating whether or not you wish to select an option. This object allows you to toggle between two choices. By clicking in this box, a check mark or an “X” is placed, indicating that you selected the option. When this box is not checked, the option is not selected.
- **control panel** - the panel that displays at the left of a screen. This panel can contain links that can be clicked to open windows or dialog boxes at the right of the screen. One or more tree lists also can display in this panel. When an item in the tree list is double-clicked, the tree list opens to reveal items that can be selected.

- **dialog box** - a box that opens in response to a command made in a window or screen, and requires your input. You must choose an option by clicking a button (such as “Yes” or “No”, or “Next” or “Cancel”) to execute your command. As dictated by this box, you also might need to make one or more entries or selections prior to clicking a button.



- **field** - an area in a dialog box, window, or screen that either accommodates your data entry, or displays pertinent information. A text box is a type of field.

Short Name

- **frame** - a boxed-in area in a dialog box, window, or screen that includes a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, check-boxes, and/or tables. Objects within a frame belong to a specific function or group. A frame often is labeled to indicate its function or purpose.

Page Content

☒ Basic

☐ Filter Info

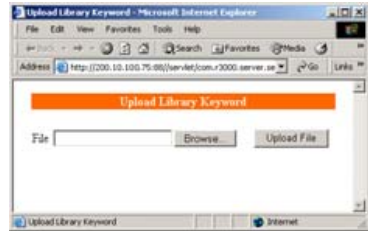
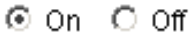
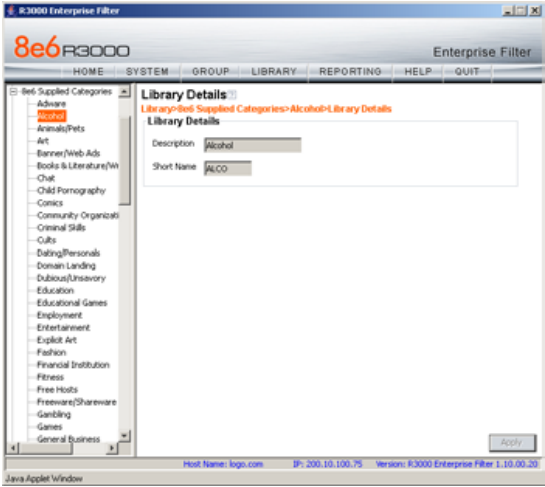
☐ Override Account

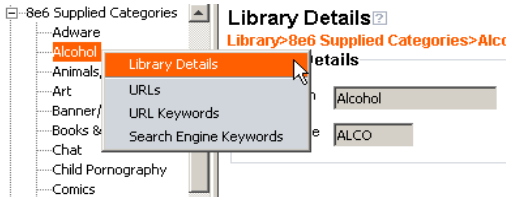
- **grid** - an area in a frame that displays rows and columns of data, as a result of various processes. This data can be reorganized in the R3000 console, by changing the order of the columns.

Date	Filename	Content	Comment
Jul 22, 2003	lib1.tar.gz	LIBRARY_ONLY	backup old library
Jul 23, 2003	config3.tar.gz	CONFIG_ONLY	backup old configurations
Jul 22, 2003	config1.tar.gz	CONFIG_ONLY	testing
Jul 22, 2003	both.tar.gz	CONFIG_AND_LIBRARY	backup library and configs

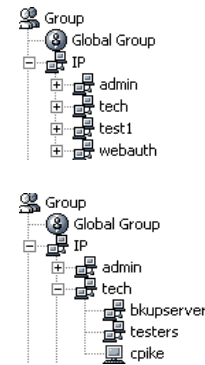
- **list box** - an area in a dialog box, window, or screen that accommodates and/or displays entries of items that can be added or removed.



- pop-up box or pop-up window** - a box or window that opens after you click a button in a dialog box, window, or screen. This box or window may display information, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.
 
- pull-down menu** - a field in a dialog box, window, or screen that contains a down-arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.
 
- radio button** - a small, circular object in a dialog box, window, or screen used for selecting an option. This object allows you to toggle between two choices. By clicking a radio button, a dot is placed in the circle, indicating that you selected the option. When the circle is empty, the option is not selected.
 
- screen** - a main object of an application that displays across your monitor. A screen can contain panels, windows, frames, fields, tables, text boxes, list boxes, icons, buttons, and radio buttons.
 

- sub-topic** - a subset of a main topic that displays as a menu item for the topic. The menu of subtopics opens when a pertinent topic link in the left panel—the control panel—of a screen is clicked. If a sub-topic is selected, the window for that sub-topic displays in the right panel of the screen, or a pop-up window or an alert box opens, as appropriate.
 
 The screenshot shows a web interface for '8e6 R3000 Enterprise Filter'. On the left, there is a list of categories under '8e6 Supplied Categories', including 'Adware', 'Alcohol', 'Animals', 'Art', 'Banner', 'Books & Chat', 'Child Pornography', and 'Comics'. The 'Alcohol' category is highlighted. A dropdown menu is open for 'Alcohol', showing options: 'Library Details', 'URLs', 'URL Keywords', and 'Search Engine Keywords'. The 'Library Details' option is highlighted. On the right, there is a 'Library Details' section with a search bar and a list of results, including 'Alcohol' and 'ALCO'.
- text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See “field”.)
- topic** - a topic displays as a link in the left panel—the control panel—of a screen. By clicking the link for a topic, the window for that topic displays in the right panel of the screen, or a menu of sub-topics opens.
 
 The screenshot shows the '8e6 R3000 Enterprise Filter' interface. The left panel, titled 'SYSTEM', contains a list of topics: 'System', 'Control', 'Network', 'Administrator', 'Diagnostics', 'Alert', 'Patch', 'Synchronization', 'Mode', 'Authentication', 'NIC Mode', 'Backup/Restore', 'Reset', 'Radius Authentication Settings', 'SNMP', 'Hardware Failure Detection', and 'X Strikes Blocking'. The 'SYSTEM' topic is highlighted. The right panel, titled 'SYSTEM', contains a description of the system section and a list of main topics. The 'SYSTEM' topic is highlighted.

- **tree** - a tree displays in the control panel of a screen, and is comprised of a hierarchical list of items. An entity associated with a branch of the tree is preceded by a plus (+) sign when the branch is collapsed. By double-clicking the item, a minus (-) sign replaces the plus sign, and any entity within that branch of the tree displays. An item in the tree is selected by clicking it.



- **window** - a window displays on a screen, and can contain frames, fields, text boxes, list boxes, buttons, checkboxes, and radio buttons. A window for a topic or sub-topic displays in the right panel of the screen. Other types of windows include pop-up windows, login windows, or ones from the system such as the Save As or Choose file windows.

Filter

System>Control>Filter

Local Filtering

Local Filtering ☒ On ☐ Off

VLAN Detection ☐ On ☒ Off

Service Blocking

Instant Messaging ☐ On ☒ Off

POP ☐ On ☒ Off

HTTPS Filtering

HTTPS Filtering Level ☐ None ☐ Low ☒ Medium ☐ High

Service Control

Proxy Pattern Blocking ☐ On ☒ Off

Target(s) Filtering

All Target(s) Filtering ☒ On ☐ Off

Filtering Elements

Filtering operations include the following elements: groups, filtering profiles and their components, and rules for filtering.

Group Types

In the Group section of the Administrator console, group types are structured in a tree format in the control panel. There are four group types in the tree list:

- **Global Group**
- **IP groups**
- **NT domain groups**
- **LDAP domain groups**



NOTE: *If authentication is enabled, the global administrator—who has all rights and permissions on the R3000 server—will see all branches of the tree: Global Group, IP, NT, and LDAP. If authentication is disabled, only the Global Group and IP branches will be seen.*

Global Group

The first group that must be set up is the global group,

represented in the tree structure by the global icon .

The filtering profile created for the global group represents the default profile to be used by all groups that do not have a filtering profile, and all users who do not belong to a group.

IP Groups

The IP group type is represented in the tree by the IP icon . A master IP group is comprised of sub-group members and/or individual IP members .

The global administrator adds master IP groups, adds and maintains override accounts at the global level, and establishes and maintains the minimum filtering level.

The group administrator of a master IP group adds sub-group and individual IP members, override account and time profiles, and maintains filtering profiles of all members in the master IP group.

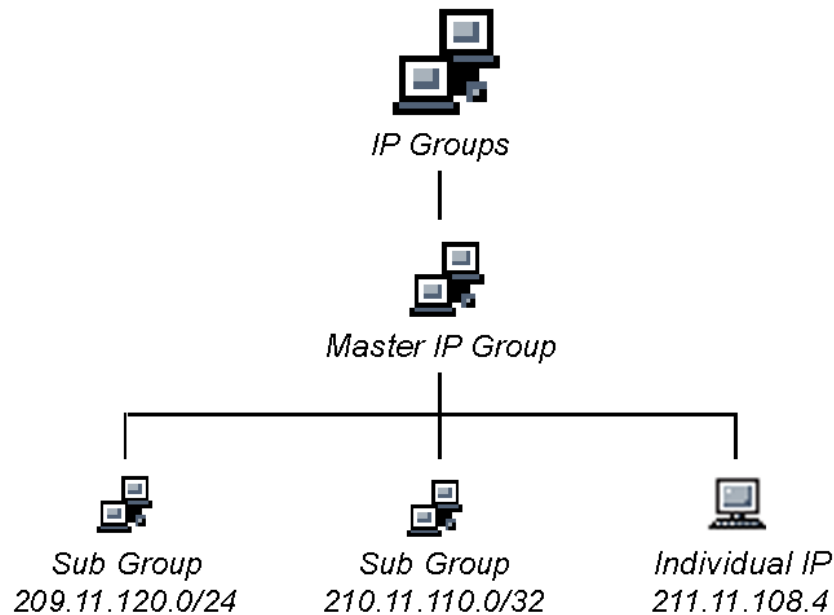


Fig. 1-1 IP diagram with a sample master IP group and its members

NT Domain Groups

An NT domain on a network server is comprised of Windows NT groups and their associated members (users), derived from profiles on the network's domain controller.

The NT group type is represented in the tree by the NT icon



. This branch will only display if authentication is enabled. Using the tree menu, the global administrator adds and maintains NT domains , and profiles of NT groups and members within the domain.

Filtering profiles can be created for a specified group  or user . If users belong to more than one group, the global administrator sets the priority for group filtering.

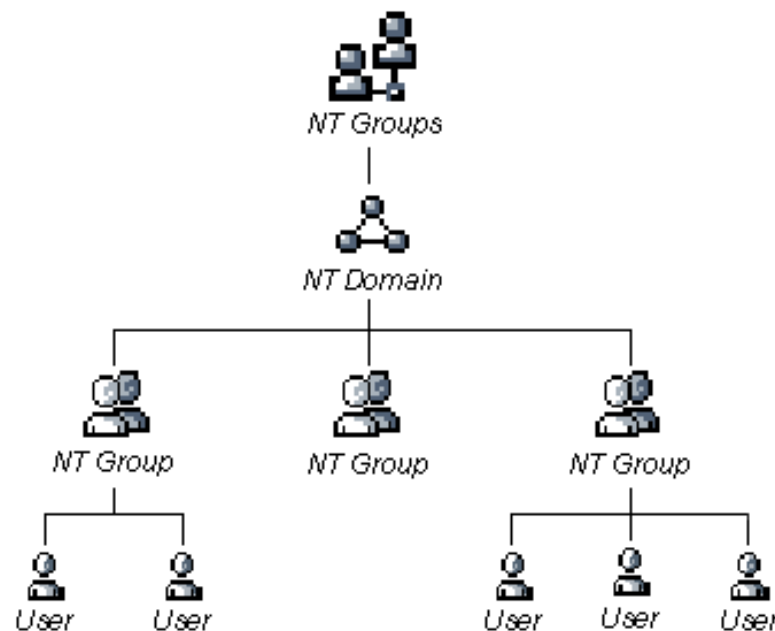


Fig. 1-2 NT domain diagram, with sample groups and members

LDAP Domain Groups

An LDAP (Lightweight Directory Access Protocol) domain on a network server is comprised of LDAP groups and their associated members (users), derived from profiles on the network's authentication server.

The LDAP group type is represented in the tree by the

LDAP icon . This branch will only display if authentication is enabled. Using the tree menu, the global administrator adds and maintains LDAP domains , and profiles of LDAP groups and members within the domain.

Filtering profiles can be created for a specified group  or user . If users belong to more than one group, the global administrator sets the priority for group filtering.

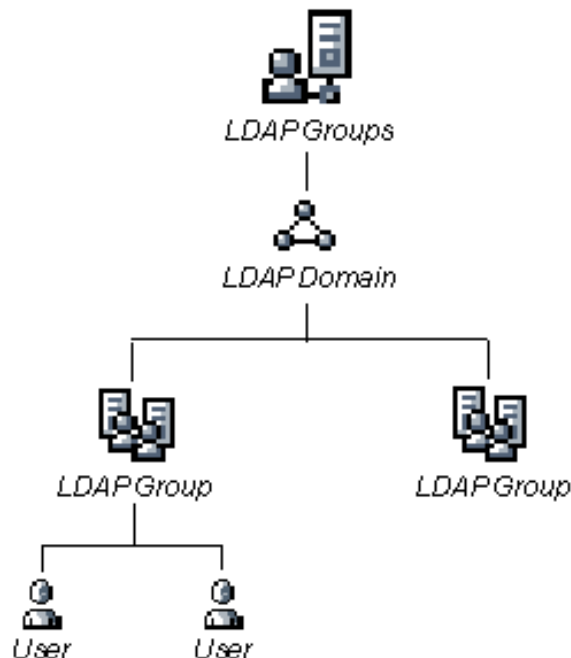


Fig. 1-3 LDAP domain diagram, with sample groups and members

Filtering Profile Types

A filtering profile is used by all users who are set up to be filtered on the network. This profile consists of rules that dictate whether a user has access to a specified Web site or service on the Internet.

The following types of filtering profiles can be created, based on the set up in the tree menu of the Group section of the console:

Global Group

- **global filtering profile** - the default filtering profile positioned at the base of the hierarchical tree structure, used by end users who do not belong to a group.

IP group (Master Group)

- **master group filtering profile** - used by end users who belong to the master group.
- **master time profile** - used by master group users at a specified time.

IP group member

- **sub-group filtering profile** - used by a sub-group member.
- **individual filtering profile** - used by an individual IP group member.
- **time profile** - used by a sub-group/individual IP group member at a specified time.

Authentication filtering profiles

- **NT/LDAP group filtering profile** - used by an NT or LDAP group.
- **NT/LDAP member filtering profile** - used by an NT or LDAP group member.

Other filtering profiles

- **override account profile** - set up in either the global group section or the master group section of the console.



NOTE: An override account set up in the master IP group section of the R3000 console takes precedence over an override account set up in the global group section of the console.

- **lock profile** - set up under X Strikes Blocking in the Filter Options section of the profile.

Static Filtering Profiles

Static filtering profiles are based on fixed IP addresses and include profiles for master IP groups and their members.

Master IP Group Filtering Profile

The master IP group filtering profile is created by the global administrator and is maintained by the group administrator. This filtering profile is used by members of the group—including sub-group and individual IP group members—and is customized to allow/deny users access to URLs, to redirect users to another URL instead of having a block page display, and to specify usage of appropriate filter options.

IP Sub-Group Filtering Profile

An IP sub-group filtering profile is created by the group administrator. This filtering profile applies to end users in an IP sub-group and is customized for sub-group members.

Individual IP Member Filtering Profile

An individual IP member filtering profile is created by the group administrator. This filtering profile applies to a specified end user in a master IP group.

Active Filtering Profiles

Active filtering profiles include the global group profile, NT/LDAP authentication profile, override account profile, time profile, and lock profile.

Global Filtering Profile

The global filtering profile is created by the global administrator. This profile is used as the default filtering profile. The global filtering profile consists of a customized profile that contains a list of library categories to block, open, or add to a white list, and service ports that are configured to be blocked. A URL can be specified for use instead of the standard block page when users attempt to access material set up to be blocked. Various filter options can be enabled.

NT/LDAP Group Filtering Profile

An NT or LDAP group filtering profile is created by the global administrator. This profile can be customized to allow/deny group users access to URLs, to redirect users to another URL instead of having the standard block page display, and to specify usage of appropriate filter options.

If users belong to more than one group, all groups to which they belong must be ranked to determine the priority each filtering profile takes over another.

NT/LDAP Member Filtering Profile

An NT or LDAP member filtering profile is created by the global administrator. This profile can be customized to allow/deny a user access to URLs, to redirect the user to another URL instead of the standard block page, and to specify usage of appropriate filter options.

Override Account Profile

If any user needs access to a specified URL that is set up to be blocked, the global administrator or group administrator can create an override account for that user. This account grants the user access to areas set up to be blocked on the Internet.

Time Profile

A time profile is a customized filtering profile set up to be effective at a specified time period for designated users.

Lock Profile

This filtering profile blocks the end user from Internet access for a set period of time, if the end user's profile has the X Strikes Blocking filter option enabled and he/she has received the maximum number of strikes for inappropriate Internet usage.



NOTE: Refer to the *R3000 User Guide* for additional information on the Override Account Profile, Time Profile, and Lock Profile.

Filtering Profile Components

Filtering profiles are comprised of the following components:

- **library categories** - used when creating a rule, minimum filtering level, or filtering profile for the global group or any entity
- **service ports** - used when setting up filter segments on the network, creating the global group (default) filtering profile, or establishing the minimum filtering level
- **rules** - specify which library categories should be blocked, left open, or white listed
- **filter options** - specify which features will be enabled: X Strikes Blocking, Google/Yahoo! Safe Search Enforcement, Search Engine Keyword Filter Control, URL Keyword Filter Control
- **minimum filtering level** - takes precedence over filtering profiles of entities who are using a filtering profile other than the global (default) filtering profile
- **filter settings** - used by service ports, filtering profiles, rules, and the minimum filtering level to indicate whether users should be granted or denied access to specified Internet content

Library Categories

A library category contains a list of Web site addresses and keywords for search engines and URLs that have been set up to be blocked or white listed. Library categories are used when creating a rule, the minimum filtering level, or a filtering profile.

8e6 Supplied Categories

8e6 furnishes a collection of library categories, grouped under the heading “8e6 Supplied Categories.” Updates to these categories are provided by 8e6 on an ongoing basis, and global administrators also can add or delete individual URLs within a specified library category.

Custom Categories

Custom library categories can be added by either global or group administrators. As with 8e6 supplied categories, additions and deletions can be made within a custom category. However, unlike 8e6 supplied categories, a custom category can be deleted.



NOTE: 8e6 cannot provide updates to custom categories. Maintaining the list of URLs and keywords is the responsibility of the global or group administrator.

Service Ports

Service ports are used when setting up filter segments on the network (the range of IP addresses/netmasks to be detected by the R3000), the global (default) filtering profile, and the minimum filtering level.

When setting up the range of IP addresses/netmasks to be detected, service ports can be set up to be open (ignored). When creating the global filtering profile and the minimum filtering level, service ports can be set up to be blocked or filtered.

Examples of service ports that can be set up include File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Network News Transfer Protocol (NNTP), Secured HTTP Transmission (HTTPS), and Secure Shell (SSH).

Rules

A rule is comprised of library categories to block, leave open, or include in a white list. Each rule that is created by the global administrator is assigned a number. A rule is selected when creating a filtering profile for an entity.

Minimum Filtering Level

The minimum filtering level consists of library categories set up at the global level to be blocked or opened, and service ports set up to be blocked or filtered. If the minimum filtering level is created, it applies to all users in IP, NT, and LDAP groups, and takes precedence over filtering settings made for group and member filtering profiles.

The minimum filtering level does not apply to any user who does not belong to a group, and to groups that do not have a filtering profile established.



NOTE: *If the minimum filtering level is not set up, global (default) filtering settings will apply instead.*

Filter Settings

Categories and service ports use the following settings to specify how filtering will be executed:

- **block** - if a category or a service port is given a block setting, users will be denied access to the item set up as “blocked”
- **open** - if a category or the filter segment detected on the network is given an open (pass) setting, users will be allowed access to the item set up as “opened”
- **always allowed** - if a category is given an always allowed setting, the category is included in the user’s white list and takes precedence over blocked categories
- **filter** - if a service port is given a filter setting, that port will use filter settings created for library categories (block or open settings) to determine whether users should be denied or allowed access to that port
- **ignore** - if the filter segment detected on the network has a service port set up to be ignored, that service port will be bypassed

Filtering Rules

Individual User Profiles - A user in an NT or LDAP domain can have only one individual profile set up per domain.

Filtering Levels Applied:

1. The global (default) filtering profile applies to any user under the following circumstances:
 - the user does not belong to a master IP group
 - the user has not been assigned a domain default profile from an NT or LDAP authentication domain
2. If a minimum filtering level is defined, it applies to all master IP groups (and their members) and NT/LDAP groups who have been assigned filtering profiles after authenticating. The minimum filtering level combines with the user's profile to guarantee that categories blocked in the minimum filtering level are blocked in the user's profile.
3. For master IP group members:
 - a. A master IP group filtering profile takes precedence over the global profile.
 - b. A master IP group time profile takes precedence over the master IP group profile.
4. For IP sub-group members:
 - a. An IP sub-group filtering profile takes precedence over the master IP group's time profile.
 - b. An IP sub-group time profile takes precedence over the IP sub-group profile.
5. For individual IP members:
 - a. An individual IP member filtering profile takes precedence over the IP sub-group's time profile.
 - b. An individual IP member time profile takes precedence over the individual IP member profile.

6. For NT/LDAP users, if a user is authenticated, settings for the user's group or individual profile from the NT/LDAP domain are applied and take precedence over any IP profile.
 - a. If the user belongs to more than one group in an authentication domain, the profile for the user is determined by the order in which the groups are listed in the Group Priority list set by the global administrator. The user is assigned the profile for the group highest in the Group Priority list.
 - b. If a user has an individual profile set up, that profile supercedes all other profile levels for that user. The user can have only one individual profile in each domain.
7. An override account profile takes precedence over an authentication profile. This account may override the minimum filtering level—if the override account was set up in the master IP group tree, and the global administrator allows override accounts to bypass the minimum filtering level, or if the override account was set up in the global group tree.



NOTE: *An override account set up in the master IP group section of the R3000 console takes precedence over an override account set up in the global group section of the console.*

8. A lock profile takes precedence over all filtering profiles. This profile is set up under Filter Options, by enabling the X Strikes Blocking feature.

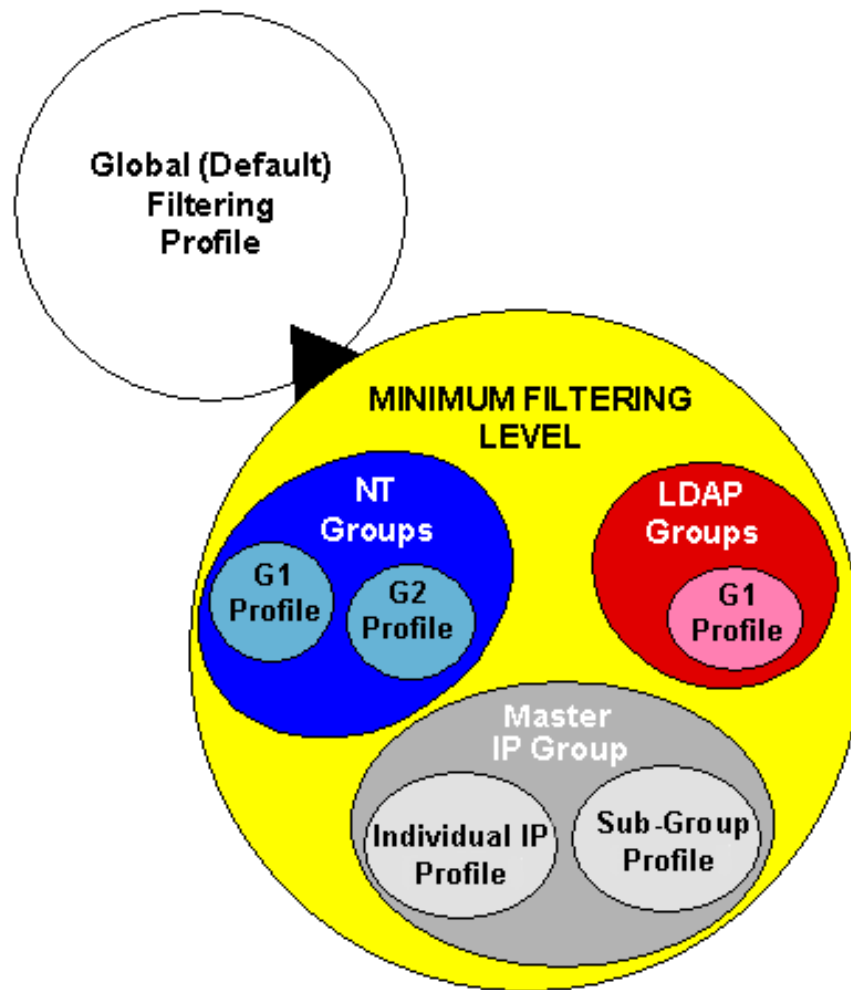


Fig. 1-4 Sample filtering hierarchy diagram

Authentication Operations

R3000 Authentication Protocols

The R3000 supports two types of authentication protocols: Windows NT LAN Manager (NTLM), and Lightweight Directory Access Protocol (LDAP).

- NTLM authentication supports NTLM authentication running on any of the following servers: Windows NT 4.0, Windows 2000 Mixed Mode, and Windows 2003 Mixed Mode.
- LDAP authentication supports all versions of LDAP, such as Microsoft Active Directory, Novell eDirectory, Sun ONE, and OpenLDAP.

R3000 Authentication Tiers

The R3000 authentication architecture for NTLM and LDAP authentication protocols is comprised of three tiers. When using NT and/or LDAP authentication with the R3000, one of these three tiers is selected for use on the network, depending on the server(s) used on the network and the preferred authentication method(s) to be employed.

- Tier 1: Single sign-on, net use based authentication for NT or Active Directory domains.
- Tier 2: Time-based, Web authentication for NT and LDAP authentication methods.
- Tier 3: Session-based, Web authentication for NT or LDAP authentication method.

When using Tier 2 or Tier 3, the 8e6 Authenticator should be enabled to ensure the end user is authenticated when logging into his/her workstation. Or if using a Novell eDirec-

tory server, the Novell eDirectory Agent can be used instead to authenticate end users.



NOTE: See *8e6 Authenticator and Novell eDirectory Agent* for information on setting up these types of authentication on the network.

Tier 1: Single Sign-On Authentication

Net use based authentication process

The following diagram and steps describe the operations of the net use based user authentication process:

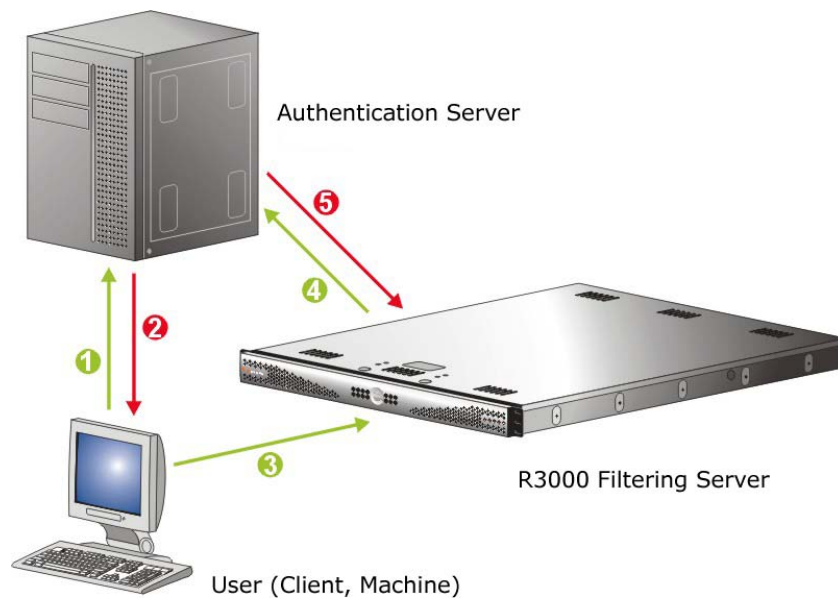


Fig. 1-5 Net use based authentication module diagram

1. The user logs on the network from a Windows workstation (also known as “client” or “machine”).
2. The authentication server on the network sends the user’s workstation a login script containing a net use command.
3. The execution of this net use command causes the Windows workstation to create an “IPC share” (command exchange) with the R3000 filter box as a shared network device.



NOTE: When the IPC share is created, no drives are mapped in this share.

4. Upon creating the IPC share, the software in the R3000 queries the network authentication server with the user's login name and password sent by the workstation.
5. Once the user is successfully authenticated, the R3000 matches the user's login name or group name with a stored list of profile settings in the R3000. As a result of this process, the user is assigned the appropriate level of filtering.
6. The matched profile is set for the user's IP address. The IPC connection is completed and maintained with periodic "keep-alives."
7. When the user logs off, changes IP addresses, loses the network connection, or in any way causes the IPC connection to be altered or deactivated, the R3000 senses this change and returns the IP address to the configured global filtering level.



WARNING: Authentication will fail if a Network Address Translation (NAT) device is set up between the authentication server and end user clients. Authentication may also fail if network connections are overloaded, causing a severe delay in the transportation of SMB traffic. This can be a problem in any network, but is most prevalent in WAN links, or in trunk links that are overloaded.

Re-authentication process

1. The user loses his/her user profile after one of the following incidences occurs:
 - the server is rebooted, or
 - the connection from the user's machine to the server is dropped (as with a faulty network cable)
2. A block page displays for the user.
3. In order to re-access the Internet, the user must re-authenticate him/herself by clicking a link in the block page to generate a login script that re-authenticates the user's profile.

Authentication methods

Tier 1 supports two server authentication methods: Server Message Block (SMB) and LDAP.

SMB protocol

SMB is a client/server protocol that requires the client to send a request to the server and receive an authentication response from the server, in order for the client to access resources on the network.

As the default protocol for NT 4.0 and earlier operating systems, SMB is supported by Windows 2000 and later OS versions.

SMB Signing

SMB Signing is a Windows security feature that prevents an active network session between a client and server from being tapped. While Microsoft has made this feature available since Windows NT 4.0, it was not a default setting. However, in Windows 2003, this feature is enabled by default.

Since SMB Signing is not currently supported by the R3000, 8e6 recommends disabling the requirement for this feature. This does not disable SMB Signing for machines that support it, but allows devices that do not support SMB Signing to connect. To disable the default setting that requires SMB Signing for all connections, follow the instructions in Appendix D: Disable SMB Signing Requirements.

Alternately, if you have an available Windows 2000 Server—or an earlier Windows NT 4.0 Server—and are willing to establish the necessary trust relationships with the Windows 2003 Server, this earlier Windows server can be used as the primary authentication server for the R3000 instead of the Windows 2003 Server.



NOTE: For information on SMB Signing compatibility with the R3000, refer to the chart in Appendix D: Disable SMB Signing Requirements.

LDAP protocol

LDAP is a directory service protocol that stores entries (Distinguished Names) in a domain's directory using a hierarchical tree structure. The LDAP directory service is based on a client/server model protocol to give the client access to resources on the network.

When a client connects to a server and asks it a question, the server responds with an answer and/or with a pointer to the server that stores the requested information (typically, another LDAP server). No matter which LDAP server the client accesses, the same view of the directory is “seen.”

The LDAP specification defines both the communication protocol and the structure, or schema, to a lesser degree. There is an Internet Assigned Network Authority (IANA) standard set that all LDAP directories should contain. Novell and Microsoft both have additional schema definitions that extend the default setups.

Most server operating systems now support some implementations of LDAP authentication. The Microsoft Active Directory LDAP-based model became available with the release of Windows 2000.

Name resolution methods

The name resolution process occurs when the R3000 attempts to resolve the IP address of the authentication server with the machine name of that server. This continuous and regulated automated procedure ensures the connection between the two servers is maintained.

When using an NT server with SMB, the name resolution process occurs when a valid Windows Internet Name Service (WINS) Server IP address is entered or a broadcast query is made.

When using an LDAP server, the name resolution process occurs when a Domain Name Service (DNS) entry is made. In order to accommodate this request, the LDAP server must have a valid DNS entry or the IP address must be added to the R3000 hosts file.



NOTE: *If LDAP is used, client machines will still use the SMB authentication method to communicate with the R3000 server for Tier 1 authentication. LDAP communication only occurs between the R3000 server and the LDAP server.*

Authentication setup procedures

Server setup types

R3000 authentication is designed to support the following server types for the specified tier(s):

Tier 1: Net use based authentication



NOTE: Login scripts must be used for net use based authentication.

Using SMB/NetBIOS:

- Windows NT 4.0, SP4 or later
- Windows 2000 or 2003 Server in mixed/legacy mode



NOTE: SMB Signing must not be required.

Using LDAP:

- Microsoft Active Directory Mixed Mode
- Microsoft Active Directory Native Mode

Tier 2 and Tier 3: Web-based authentication

Using an NT authentication domain:

- Windows NT 4.0, SP4 or later
- Windows 2000 or 2003 Server in mixed/legacy mode



NOTE: SMB Signing must not be required.

Using an LDAP domain:

- Windows Active Directory 2002 and 2003
- Novell eDirectory
- SunONE directory server

Configuring the authentication server

When configuring authentication, you must first go to the authentication server and make all necessary entries before configuring the R3000.

The following authentication components must be set up or entered on the console of the authentication server:

- domain name
- usernames and passwords
- user groups
- login scripts

Login scripts

Login (or logon) scripts are used by the R3000 server for reauthenticating users on the network.

The following syntax must be entered in the appropriate directory on the authentication server console:

Enter net use syntax in the login script

The virtual IP address is used by the R3000 to communicate with all users who log on to that server. This address must be in the same subnet as the one used by the transmitting interface of the R3000.

- For testing, user information can be specified on the command line as follows:

NET USE \\virtualip\R3000\$ /user:DOMAIN-NAME\username password

Example: NET USE \\192.168.0.20\R3000\$/user:LOGO\jsmith xyz579

- The command to disconnect a session is:

NET USE \\virtualip\R3000\$ /delete

View login script on the server console

The login script can be viewed on the authentication server console. This script resides in a different location on the server, depending on the version of the server:

- **Windows 2000 or Windows 2003 Server**

\\servername.suffix\sysvol\domainname.suffix\
policies\{guid}\user\scripts\logon

c:\winnt\sysvol\sysvol\domainname.suffix\scripts

c:\winnt\sysvol\domainname\scripts

- **Windows NT 4.0 Server**

\\servername\netlogon

\\ipaddress\netlogon

c:\winnt\system32\repl\import\scripts

The login script must be specified either in the user's domain account or in the Active Directory Group Policy Object so that it runs when the user logs into the domain.

Block page authentication login scripts

In addition to the use of login scripts in the console of the authentication server, a login script path must be entered in the Block Page window of the R3000 Administrator console. This script is used for reauthenticating users on the network.

The following syntax must be used:

\\SERVERNAME\netlogon

or

\\IPaddress\netlogon



NOTE: See *Block Page Authentication* for more information about these entries.

LDAP server setup rules



WARNING: *The instructions in this user guide have been documented based on standard default settings in LDAP for Microsoft Active Directory Services. The use of other server types, or any changes made to these default settings, must be considered when configuring the R3000 server for authentication.*

If LDAP will be used, the following items should be considered:

- The administrator in charge of the LDAP server should create a user for the R3000 in order to give that user full read access to the groups and users in the directory.
- Since the LDAP directory is structured as a tree, data needs to be retrieved the same way. Additionally, the order of the syntax is reversed compared to how it appears in normal file system folders. The deepest layer is listed first, in a similar manner as a DNS domain name: e.g. “engineering.company.net”. In LDAP, a directory entry would look like this: “cn=engineering,dc=company,dc=net”.
- Make sure all network configuration settings are correct (such as DNS, IP, etc.) before configuring LDAP settings.



NOTE: *All filtering profiles are stored on the R3000 server.*

Tier 2: Time-based, Web Authentication

The following diagram and steps describe the operations of the time-based authentication process:

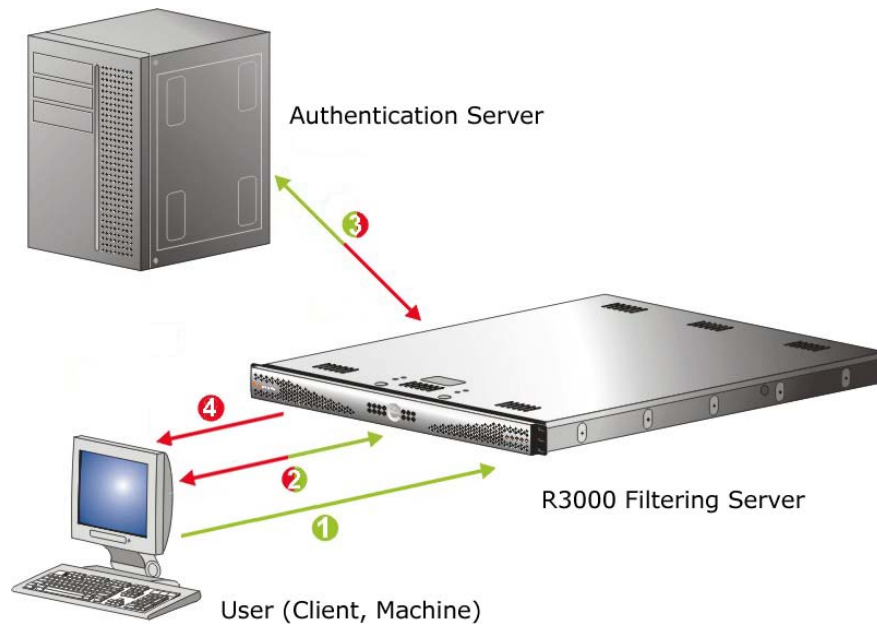


Fig. 1-6 Web-based authentication module diagram

1. The user makes a Web request by entering a URL in his/her browser window.
2. The R3000 intercepts this request and sends the user the Authentication Request Form, requesting the user to log in with his/her login ID and password.
3. The R3000 verifies the user's information with the authentication server (Domain Controller, Active Directory, LDAP, etc.).
4. The authenticated user is allowed to access the requested URL for the time period specified by the administrator.

Tier 2 implementation in an environment

In an environment where Tier 2 time-based profiles have been implemented, end users receive filtering profiles after correctly entering their credentials into a Web-based Authentication Request Form. A profile remains active for a configurable amount of time even if the user logs out of the workstation, changes IP addresses, etc.

Tier 2 time-based profiles do not call for the R3000 to maintain a connection with the client machine, so the R3000 cannot detect when the user logs off of a workstation. In order to remove the end user's profile, one of two scripts detailed in this sub-section should be inserted into the network's login and/or logoff script.

The Tier 2 Script should be used if Tier 2 is the only tier implemented in an environment. The Tier 1 and Tier 2 Script should be used if Tier 2 is implemented along with Tier 1 in an environment. Since both sets of scripts use the NET USE command, the client machine must already have the ability to connect to the R3000 via NET USE in order for the profile to be removed in either environment.

Tier 2 Script

If using Tier 2 only, this script should be inserted into the network's login script. If the network also uses a logoff script, 8e6's script should be inserted there as well. The inclusion of this script ensures that the previous end user's profile is completely removed, in the event the end user did not log out successfully.

```
echo off
:start
cls
net use \\10.10.10.10\LOGOFF$ /delete

:try1
NET USE \\10.10.10.10\LOGOFF$
if errorlevel 1 goto :try2
if errorlevel 0 echo code 0: Success
goto :end

:try2
NET USE \\10.10.10.10\LOGOFF$
if errorlevel 1 goto :try3
if errorlevel 0 echo code 0: Success
goto :end

:try3
NET USE \\10.10.10.10\LOGOFF$
if errorlevel 1 goto :error
if errorlevel 0 echo code 0: Success
goto :end

:error
if errorlevel 1 echo code 1: Failed!

:end
net use \\10.10.10.10\LOGOFF$ /delete
```


Tier 1 and Tier 2 Script

In an environment in which both Tier 1 and Tier 2 are used, this version of 8e6's script should be inserted into the network's login script. 8e6's script attempts to remove the previous end user's profile, and then lets the new user log in with his/her assigned profile.

```
echo off
:startremove
cls
NET USE \\10.10.10.10\LOGOFF$ /delete

:tryremove1
NET USE \\10.10.10.10\LOGOFF$
if errorlevel 1 goto :tryremove2
if errorlevel 0 echo code 0: Success
goto :endremove

:tryremove2
NET USE \\10.10.10.10\LOGOFF$
if errorlevel 1 goto :tryremove3
if errorlevel 0 echo code 0: Success
goto :endremove

:tryremove3
NET USE \\10.10.10.10\LOGOFF$
if errorlevel 1 goto :removalerror
if errorlevel 0 echo code 0: Success
goto :endremove

:removalerror
if errorlevel 1 echo code 1: Failed to send removal
request!

:endremove
net use \\10.10.10.10\LOGOFF$ /delete
```

```
:try1
NET USE \\10.10.10.10\R3000$
if errorlevel 1 goto :try2
if errorlevel 0 echo code 0: Success
goto :end

:try2
NET USE \\10.10.10.10\R3000$
if errorlevel 1 goto :try3
if errorlevel 0 echo code 0: Success
goto :end

:try3
NET USE \\10.10.10.10\R3000$
if errorlevel 1 goto :error
if errorlevel 0 echo code 0: Success
goto :end

:error
if errorlevel 1 echo code 1: Failed!

:end
```

in environments that use both Tier 1 and Tier 2, if a logoff script is used on the network, the Tier 2 Script should be inserted into the network's logoff script.

Tier 3: Session-based, Web Authentication

The diagram on the previous page (Fig. 1-6) and steps below describe the operations of the session-based authentication process:

1. The user makes a Web request by entering a URL in his/her browser window.
2. The R3000 intercepts this request and sends the user the Authentication Request Form, requesting the user to log in with his/her login ID and password.
3. The R3000 verifies the user's information with the authentication server (Domain Controller, Active Directory, LDAP, etc.).
4. A pop-up window opens on the user's workstation while the original window loads the requested URL. The user will continue to be authenticated as long as the pop-up window remains open.

8e6 Authenticator

The 8e6 Authenticator ensures the end user is authenticated on his/her workstation, via an executable file that launches during the login process. To use this option, the 8e6 Authenticator client (`authenticat.exe`) should be placed in a network share accessible by the domain controller or a Novell eDirectory server such as NetWare eDirectory server 6.5.



NOTE: The 8e6 Authenticator client (`authenticat.exe`) can be downloaded from the *Enable/Disable Authentication* window. (See the *Enable authentication, specify criteria* sub-section in Chapter 2: Network Setup.)

Environment requirements

Minimum system requirements

The following minimum server components are required when using NetWare eDirectory server 6.5:

- Server-class PC with a Pentium II or AMD K7 processor
- 512 MB of RAM
- Super VGA display adapter
- DOS partition of at least 200 MB and 200 MB available space
- 2 GB of available, unpartitioned disk space outside the DOS partition for volume sys:
- One network board
- CD drive

Recommended system requirements

The following server components are recommended for optimal performance when using NetWare eDirectory server 6.5:

- Server-class PC with two-way Pentium III, IV, or Xeon 700 MHz or higher processors
- 1 GB of RAM
- VESA compliant 1.2 or higher display adapter
- DOS partition with 1 GB of available space
- 4 GB of available, unpartitioned disk space outside the DOS partition for volume sys:
- One or more network boards
- Bootable CD drive that supports the El Torito specification
- USB or PS/2* mouse

Workstation requirements

The 8e6 Authenticator client works with the following operating systems:

- Windows XP Pro SP1 and 2
- Windows 2000 Pro SP4
- Windows XP and Windows 2000 with Novell client v4.91



NOTE: Any non-domain supported Windows operating system, such as ME or XP Home Edition, will not work with the 8e6 Authenticator unless the Novell eDirectory client is installed for login and deployment of the 8e6 Authenticator client using a Novell server.

Work flow in a Windows environment

1. The administrator stores the 8e6 Authenticator client (authenticat.exe) in a network-shared location that a login script can access.
2. Using a Windows machine, an end user logs on the domain, or logs on the eDirectory tree via a Novell client.
3. The end user's login script evokes authenticat.exe.
4. The 8e6 Authenticator client determines the authentication environment by examining the Windows registry, then retrieves the username and domain name using either Windows or Novell APIs, and sends this information (LOGON event) to the R3000.
5. The R3000 looks up the groups to which the end user belongs (Windows AD, PDC, or eDirectory through LDAP or NTLM/Samba), and determines the profile assignment.
6. The R3000 sets the profile for the end user with username (including the group name, if it is available) and IP.
7. The 8e6 Authenticator client continually sends a "heartbeat" to the R3000—with a specified interval of seconds between each "heartbeat"—until the end user logs off.
8. The end user logs off, and the 8e6 Authenticator client sends a LOGOFF event to the R3000. The R3000 removes the user's profile.



NOTE: The 8e6 Authenticator can handle up to 20 logons per second.

8e6 Authenticator configuration priority

The source and order in which parameters are received and override one another are described below.



NOTE: Any parameter set at the end of the list will override any parameter that was previously set.

1. **Compiled Defaults:** Given no parameters at all, the client will try to execute using the default compilation.
2. **Configuration File** (optional): The default location of the configuration file is the same path/name as the authenticat.exe client, but with a “.cfg” extension instead of “.exe”. The full path/name can be specified on the command line with the CF[] parameter. Review the ++ comment following Table 1 for more information.
3. **Command Line** (optional): Options on the command line will override compiled defaults and the configuration file. The command line can be left blank.
4. **R3000 Configuration Packet** (optional): The R3000 may send a configuration packet that will override all other settings, including the command line. If the R3000 changes the IP address or port used by authenticat.exe, then when authenticat.exe reconnects, authenticat.exe will use the new IP address and port.



NOTE: The R3000 can force authenticat.exe to reconnect with a re-logon event packet.

8e6 Authenticator configuration syntax

All configuration parameters, regardless of their source, will use the following format/syntax:

wAA[B]w{C}w

{Parameter 'AA' with Data 'B', and Comment 'C' ignored.}

w;DD[E]w{C}w

{The semicolon causes 'DD[E]' to be ignored, 'C' is also ignored.}

Whereas '**AA**' is a two-letter, case-insensitive parameter name, '**B**' is the value for this parameter wrapped in brackets ([]), and '**w**' is zero or more white spaces (space, tab, carriage return, line feed). '**C**' is completely ignored, and anything wrapped in braces ({ }) is considered a comment. A ';' immediately preceding a parameter will cause that parameter and its data to be ignored, which is convenient for temporarily reverting a parameter to default values during testing.

Sample command line parameters

```
authenticat.exe LF[c:] ra[192.168.0.43]Rr[40000]
```

Sample configuration file

```
RA[100.10.101.30] { R3000 Virtual IP address }
RP[139] { R3000 Port }
RH[30000] { Heartbeat timer (30 seconds) }
RR[30000] { Reconnect time (before connecting again) }
RC[10000] { Connect Timeout (how long to wait for a connection
response) }
LE[0]
LF[\\100.10.101.117\publogs\] { Where to put logs }
```

Sample R3000 configuration update packet 'PCFG'

After decryption, with protocol headers removed:

```
RH[30000]RC[1000]LE[1]
```


You only need to change the options you do not wish to remain as default. Often the IP address of the R3000 (RA) and the log file (LF) are the most desired options to change. Note that full network paths are allowed.

Table of parameters

The following table contains the different parameters, their meanings, and possible values.

Param ID	Parameter Meaning	Values	Dbg Default	Release Default
UT+	User's Logon Environment	1-256 (0 = Win32, 1 = Novell)	255 (auto)	255 (auto)
RA # *	R3000 Virtual IP Address	255.255.255.255:PORT;...	0.0.0.0	0.0.0.0
RV #	R3000 VPN Support Table	(IP-IP;IP:PORT;...),...		
RP	R3000 Port	1-65535	139	139
RH	R3000 Heartbeat Timer MS	1-4 billion (milliseconds)	30000	30000 (30 sec)
RR	R3000 Reconnect Time MS	1-4 billion (milliseconds)	30000	30000 (30 sec)
RC	R3000 Connect Timeout MS	1-4 billion (milliseconds)	10000	10000 (10 sec)
LE	Log using Event Viewer	1 or 0 (event view or log file)	0 (log file)	1 (event view)
LD	Logging Detail	1, 2, 3, or 4	1 (light)	0 (errors only)
LF *	Path-ONLY to output log file	1-1000 alphanum	C:\	C:\
CF ++	Full path/name of Configuration File	1-1000 alphanum	—	—

- + If UT[0] is set, then the Novell environment will be ignored, if present, and only the Windows environment information will be retrieved and sent to the R3000. If UT[1] is set and the Novell environment is invalid or the user is not authenticated with its Novell server, then the results sent to the R3000 are invalid (probably empty values). The default UT[255] auto detects Novell vs. Win32 and will automatically favor Novell authentication over Windows, if possible.
- * Special Interest. Values most likely to change during testing, configuration, and production implementation.
- ++ Alternate configuration file is only valid when specified on the command line. It will be ignored in any other context. If the configuration file cannot be loaded from the alternate location, an error will be logged and an attempt will be made to load the default configuration file. If the alternate configuration file is specified and is blank (CF[]), the 8e6 Authenticator will *not* attempt to load any configuration file; this can minimally speed up execution time. The compiled default value of CF[-] causes the default configuration file loading to be attempted, which has the same full path and filename of the current, loaded 8e6 Authenticator executable, but with an extension of “.cfg” instead of “.exe”. That is, if the 8e6 Authenticator client is “\\example\\authenticat.exe”, the search for the default configuration file would be “\\example\\authenticat.cfg”. It is *not* an error if the default configuration file does not exist. It *is* an error if the default configuration file exists but cannot be read or parsed correctly. Unknown parameters are ignored. Format/syntax errors will abort the reading and report an error, but the 8e6 Authenticator will attempt to continue running.
- For each IP address where “:PORT” is omitted from the address, the RP[] port value is used. For example, if RA[1.1.1.1:5555] is set, the RP[] parameter is ignored.

RP[] affects port-less addresses specified in the RV[] command as well.

- For RA[], each IP address is separated by a semi-colon ';' and the first IP address will be tried for each new connection attempt. When the main IP address fails to respond, the next IP address in the list will be tried, and so on, if it fails. After the last IP address is tried, the logic will continue from the first IP address again. A retry attempt on the main IP address is subject to the RR[] Reconnect time. After any disconnection, the logic will always begin with the main IP address as its first attempt.
- For RV[], sets of R3000 addresses are specified based on an IP range that matches the client's IP address; multiple destination R3000 addresses may be used in each set and will have the same functionality as multiple destinations specified in the RA[] parameter. Each set is surrounded by parentheses '()'s, and sets are separated by commas ','. Any local client IP address that does not match any set will use the RA[] address. Sample format:

```
RV[(102.108.1.0-102.108.1.255;1.1.1.1;2.2.2.2),(102.108.2.0-102.108.2.255;3.3.3.3:222)]
```

In this example, a client with an IP address of 102.108.1.5 would try to connect to 1.1.1.1 using the RP[] port (2.2.2.2 as the backup). A client with 192.168.2.15 would try to connect to 3.3.3.3 port 222, which has no backup.

- Any local address that would end up connecting to 0.0.0.0 will not be observed by the 8e6 Authenticator. This allows RV[] to allow only specified ranges of IP addresses to be observed by the 8e6 Authenticator.

Novell eDirectory Agent

Novell eDirectory Agent provides Single Sign-On (SSO) authentication for an R3000 set up in a Novell eDirectory environment. Using Novell eDirectory Agent, the R3000 is notified by the eDirectory server when an end user logs on or off the network, and adds/removes his/her network IP address, thus setting the end user's filtering profile accordingly.

Environment requirements

Novell eDirectory servers

The following eDirectory versions 8.7 or higher with Master, Read/Write, Read replicas have been tested:

- eDirectory 8.7 in RedHat Linux 9.0
- eDirectory 8.7 in NetWare 6.5 SP5



NOTE: See *8e6 Authenticator: Environment requirements for Minimum and Recommended system requirements*. These requirements also apply to eDirectory 8.7 in RedHat Linux 9.0.

Client workstations

To use this option, all end users must log in the network. The following OS have been tested:

- Windows 2000 Professional
- Windows XP
- Macintosh

Novell clients

The following Novell clients have been tested:

- Windows: Version 4.91 SP2
- Macintosh: Prosoft NetWare client Version 2.0

Novell eDirectory setup

The eDirectory Agent uses the LDAP eDirectory domain configuration setup in the R3000 Administrator console. The eDirectory Agent receives notification from the eDirectory server regarding logon and logoff events by end users. The Novell client must be installed on each end user's workstation in order to handle logons to the eDirectory network. In this setup, the Novell client replaces the Windows logon application.

R3000 setup and event logs

When using a Novell eDirectory server and choosing to use the Novell eDirectory Agent option in the R3000:

- Enable Novell eDirectory Agent in the Enable/Disable Authentication window.



NOTES: *If using an SSO authentication solution, Tier 2 or Tier 3 should be selected as a fallback authentication operation.*

When choosing the Novell eDirectory Agent option, the 8e6 Authenticator option must be disabled.

- If applicable, a back up server can be specified in the LDAP domain setup wizard, in the event of a connection failure to the primary Novell eDirectory server. Email alerts are sent to the administrator in such events.



NOTE: *Back up server settings are made in the Default Rule tab of the LDAP Domain Details window, described in Chapter 4: LDAP Authentication Setup.*

- Once the Novell eDirectory Agent option is set up, the View Log File window can be used to view end user logon/logoff events and the debug log.



NOTE: *After the Novell eDirectory Agent is enabled, an individual's username will not display in the event log until he/she logs in again. Until that time, the user will be logged by his/her current filtering profile, which most likely would be IPGROUP or DEFAULT user.*

Authentication Solution Compatibility

Below is a chart representing the authentication solution compatibility for a single user:

	Tier1 net use	Tier 2 time based	Tier 3 session based	8e6 Authenticator	eDirectory Agent
Tier 1	--	Yes	Yes	N/R	N/A
Tier 2	Yes	--	N/A	Yes	Yes
Tier 3	Yes	N/A	--	Yes	Yes
8e6 Authenticator	N/R	Yes	Yes	--	N/R
eDirectory Agent	N/A	Yes	Yes	N/R	--

KEY:

- N/A = Not Applicable
- N/R = Not Recommended

Configuring the R3000 for Authentication

Configuration procedures

When configuring the R3000 server for authentication, settings must be made in System and Group windows in the Administrator console.



NOTES: *If the network has more than one domain, the first one you add should be the domain on which the R3000 resides.*

The entries described in this section represent entries to be made on a typical network.

System section

The first settings for authentication must be made in the System section of the Administrator console in the following windows: Operation Mode, LAN Settings, Enable/Disable Authentication, Authentication Settings, Authentication SSL Certificate (if Web-based authentication will be used), and Block Page Authentication.

1. Select “Mode” from the control panel, and then select “Operation Mode” from the pop-up menu.

The entries made in the Operation Mode window will vary depending on whether you will be using the invisible mode, or the router or firewall mode.

In the Listening Device frame, set the Listening Device to “eth0”.

In the Block Page Device frame:

- If using the invisible mode, select “eth1”.
 - If using the router or firewall mode, select “eth0”.
2. Select “Network” from the control panel, and then select “LAN Settings” from the pop-up menu.

The entries made in this window will vary depending on whether you are using the invisible mode, or the router or firewall mode. The LAN 1 and LAN 2 IP addresses should usually be in a different subnet.

- If using the invisible mode: For the LAN1 IP (eth0) address, select 255.255.255.255 for the subnet mask.
 - If using the router or firewall mode: Specify the appropriate IP address and subnet mask in the applicable fields.
3. Select “Authentication” from the control panel, and then select Enable/Disable Authentication from the pop-up menu.

Enable authentication, and then select one of three tiers in the Web-based Authentication frame:

- Tier 1: Choose this option if you will only be using net use based authentication for NT or Active Directory servers.
 - Tier 2: Choose this option if you wish to use timed Web-based authentication for NT and LDAP domains. This option gives the user a timed session for his/her Internet access. After the timed profile expires, the user will have to log in again if he/she wants to continue to have Internet access.
 - Tier 3: Choose this option if you wish to use persistent Web-based authentication for NT and LDAP domains. This option gives the user a persistent network connection via a pop-up window that keeps the user’s session open until the window is closed, so the user does not have to log in repeatedly.
- If choosing Tier 2 or Tier 3, enable either 8e6 Authenticator or Novell eDirectory Agent, as appropriate to your environment.
4. Select “Authentication” from the control panel, and then select “Authentication Settings” from the pop-up menu.

In the Settings frame, enter general configuration settings for the R3000 server such as IP address entries.

In the NIC Device to Use for Authentication field:

- If using the invisible mode: Enter *eth1* (Ethernet 1) as the device to send traffic on the network.
- If using the router or firewall mode: Enter *eth0* (Ethernet 0).

Information should only be entered in the NT Authentication Server Details frame if the R3000 will use the NT Authentication method to authenticate users.

5. Select “Authentication” from the control panel, and then select Authentication SSL Certificate from the pop-up menu. This option should be used if Web-based authentication will be deployed on the R3000 server.

Using this option, you create either a self-signed certificate or a Certificate Request (CSR) for use by the Secure Sockets Layer (SSL). The certificate should be placed on client machines so that these machines will recognize the R3000 as a valid server with which they can communicate.

6. Select “Control” from the control panel, and then select “Block Page Authentication” from the pop-up menu.

In the Block Page Authentication window, select the Re-authentication Options to be used. The items you select will be listed as options for re-authentication on the Options page, accessible from the standard block page. If the “Re-authentication” (NET USE) option is selected, enter the login script path to be used by the R3000 for re-authentication purposes.

Group section

In the Group section of the Administrator console, choose NT or LDAP, and then do the following:

1. Add a domain from the network to the list of domains that will have users authenticated by the R3000.



NOTE: *If the network has more than one domain, the first one you add should be the domain on which the R3000 resides.*

2. Create filtering profiles for each group within that domain.
3. Set the group priority by designating which group profile will be assigned to a user when he/she logs in. If a user is a member of multiple groups, the group that is positioned highest in the list is applied.
4. Create unique filtering profiles for individual users.

CHAPTER 2: NETWORK SETUP

Environment Requirements

Workstation Requirements

Administrator

Minimum system requirements for the administrator include the following:

- Windows 98 or later operating system (not compatible with Windows server 2003)
- Internet Explorer (IE) 5.5 or later
- JavaScript enabled
- Java Virtual Machine
- Java Plug-in (use the version specified for the R3000 software version)
- Java Runtime Environment, if using Tier 3 authentication

End User

- Windows 98 or later operating system (not compatible with Windows server 2003)
- Internet Explorer (IE) 5.5 or later
- JavaScript enabled
- Java Runtime Environment, if using Tier 3 authentication
- Pop-up blocking software, if installed, must be disabled

Network Requirements

- High speed connection from the R3000 server to the client workstations
- FTP or HTTPS connection to 8e6's patch server
- Internet connectivity for downloading Java Virtual Machine—and Java Runtime Environment, if necessary—if not already installed

Set up the Network for Authentication

The first settings for authentication must be made in the System section of the console in the following windows: Operation Mode, LAN Settings, Enable/Disable Authentication, Authentication Settings, Authentication SSL Certificate (if Web-based authentication will be used), View Log File (for troubleshooting authentication setup), and Block Page Authentication. Entries for customizing the block page and/or authentication request form are made in the Common Customization, Authentication Form Customization, and Block Page Customization windows.

Specify the operation mode

Click Mode and select Operation Mode from the pop-up menu to display the Operation Mode window:

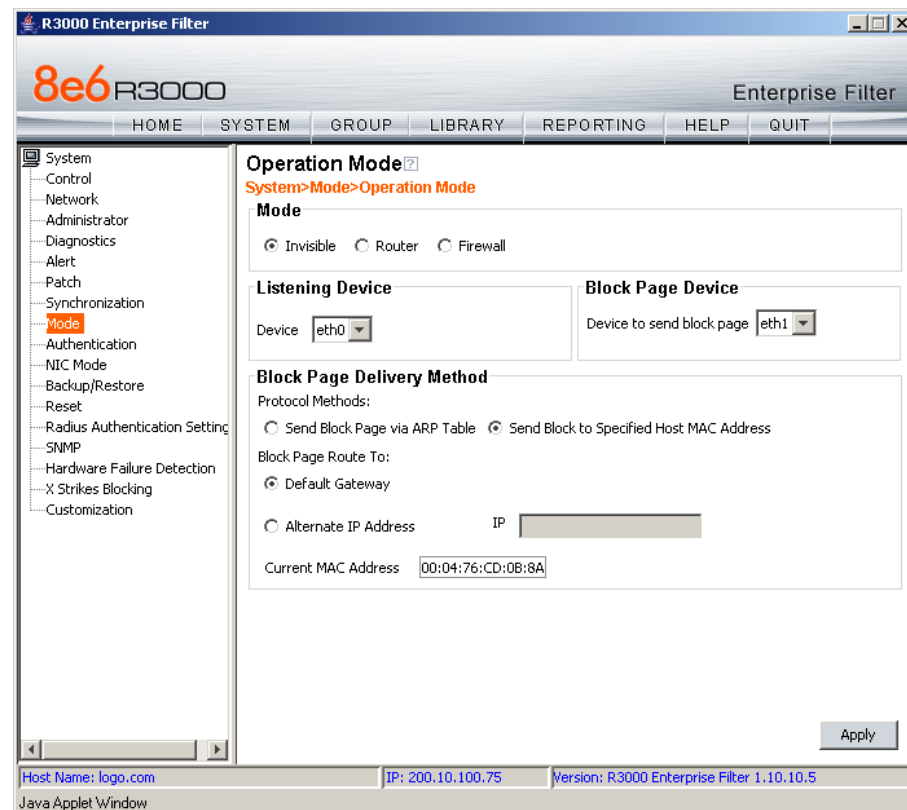


Fig. 2-1 Operation Mode window

The entries made in this window will vary depending on whether you will be using the invisible mode, or the router or firewall mode.

1. In the Mode frame, select the mode to be used: “Invisible”, “Router”, or “Firewall”.
2. In the Listening Device frame, set the **Device** to “eth0”.
3. In the Block Page Device frame:

- If using the invisible mode, select “eth1”.
- If using the router or firewall mode, select “eth0”.

If using the invisible mode, the Block Page Delivery Method frame displays. Choose from either of the two **Protocol Methods**:

- “Send Block Page via ARP Table” - this option uses the Address Resolution Protocol method to find the best possible destination MAC address of a specified host, usually the R3000 gateway.
- “Send Block to Specified Host MAC Address” - using this preferred method, the block page will always be sent to the MAC address of a specified host, usually the R3000 gateway.

Choose from either of the two **Block Page Route To** selections:

- “Default Gateway” - this option indicates that the default gateway on your network will be used for sending block pages.
- “Alternate IP Address” - this option should be used if block pages are not being served.

Enter the **IP** address of the router or device that will serve block pages.

4. Click **Apply**.

Specify the subnet mask, IP address(es)

Click Network and select LAN Settings from the pop-up menu to display the LAN Settings window:

R3000 Enterprise Filter

8e6 R3000 Enterprise Filter

HOME SYSTEM GROUP LIBRARY REPORTING HELP QUIT

System
Control
Network
Administrator
Diagnostics
Alert
Patch
Synchronization
Mode
Authentication
NIC Mode
Backup/Restore
Reset
Radius Authentication Setting
SNMP
Hardware Failure Detection
X Strikes Blocking
Customization

LAN Settings
System>Network>LAN Settings

Host Name: R3000LDAP-ota

IP / Mask Setting

LAN1 IP (eth0): 1.2.3.4 / 255.255.255.255

LAN2 IP (eth1): 190.160.20.75 / 255.255.0.0

DNS

Primary IP: 190.160.20.1

Secondary IP:

Gateway

Gateway IP: 190.160.20.1

Apply

Host Name: logo.com IP: 200.10.100.75 Version: R3000 Enterprise Filter 1.10.00.24

Java Applet Window

Fig. 2-2 LAN Settings window

The entries made in this window will vary depending on whether you are using the invisible mode, or the router or firewall mode.



NOTE: If the gateway IP address on the network changes, be sure to update the Gateway IP address in this window.

Invisible mode

For the **LAN1 IP (eth0)** address, select 255.255.255.255 for the subnet mask, and click **Apply**.

Router or firewall mode

1. Enter the following information:

- In the **LAN1 IP (eth0)** field of the IP/Mask Setting frame, enter the IP address and specify the corresponding subnet of the “eth0” network interface card to be used on the network.
- In the **LAN2 IP (eth1)** field, enter the IP address and specify the corresponding subnet of the “eth1” network interface card to be used on the network.



TIP: The LAN1 and LAN2 IP addresses should usually be placed in different subnets.

- In the **Primary IP** field of the DNS frame, enter the IP address of the first DNS server to be used for resolving the IP address of the authentication server with the machine name of that server.
- In the **Secondary IP** field of the DNS frame, enter the IP address of the second DNS server to be used for resolving the IP address of the authentication server with the machine name of that server.
- In the **Gateway IP** field of the Gateway frame, enter the IP address of the default router to be used for the entire network segment.

2. Click **Apply** to apply your settings.



NOTE: Whenever modifications are made in this window, the server must be restarted in order for the changes to take effect.

Enable authentication, specify criteria

1. Click Authentication and select Enable/Disable Authentication from the pop-up menu to display the Enable/Disable Authentication window:
2. Click **Enable** to enable authentication.
3. Select one of three tiers in the Web-based Authentication frame:

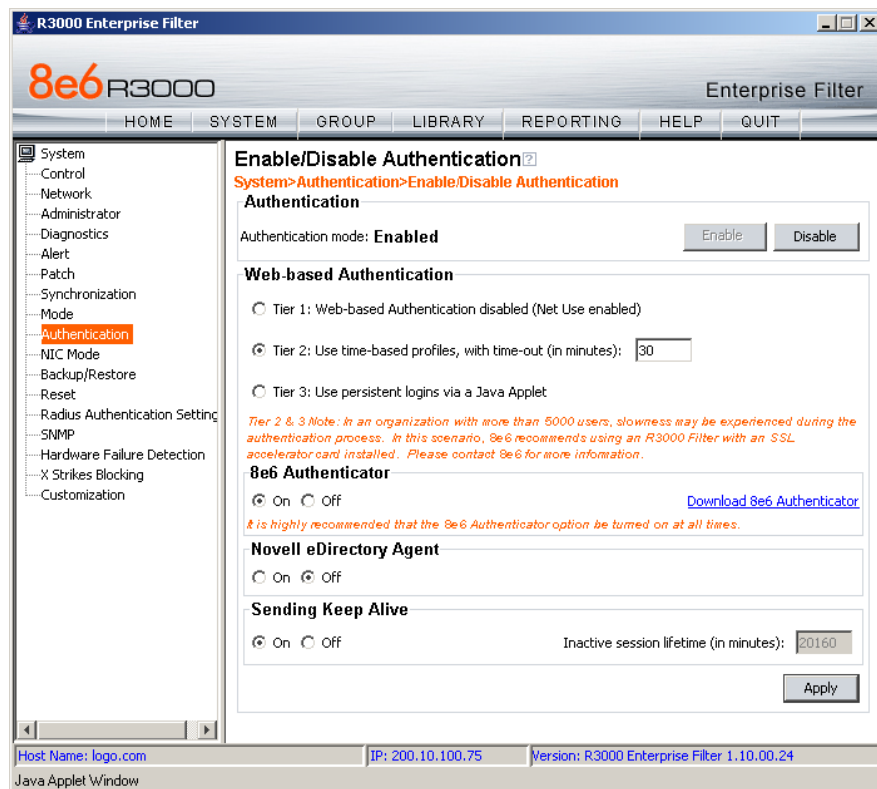


Fig. 2-3 Enable/Disable Authentication window



NOTE: See the information on the next pages for details about each of the tiers, and for the steps that must be executed to enable your tier selection.

4. In the 8e6 Authenticator frame, be sure the 8e6 Authenticator is “On”—unless the Novell eDirectory Agent option will be used instead. When enabling the 8e6 Authenticator option, and then downloading and installing the 8e6 Authenticator (authenticat.exe) on a network share accessible by the domain controller or a Novell eDirectory server, the 8e6 Authenticator automatically authenticates the end user when he/she logs into his/her workstation.
5. If you have a Novell eDirectory server and the 8e6 Authenticator will not be used, turning “On” Novell eDirectory Agent will enable end user logon and logoff events to be logged. To use this option, the LDAP domain must be set up and activated in the Group tree.



WARNING: *When enabling Novell eDirectory Agent, the agent will immediately begin scanning Novell eDirectory-based domain labels.*

6. If using Tier 1, in the Sending Keep Alive frame, click "On" to specify that keep alives should be sent on a connection to verify whether it is still active. Click "Off" to specify that the end user's session will be kept alive based on the number of minutes entered in the text box.
7. Click **Apply**.

Net use based authentication

Tier 1: Web-based Authentication disabled (Net Use enabled) – Choose this option if you will be using net use based authentication for NT or Active Directory.

1. Click “Tier 1”.
2. In the Sending Keep Alive frame, click the radio button corresponding to the option to be used:
 - “On” - This option specifies that keep alives should be sent on a connection to verify whether it is still active.
 - “Off” - This option specifies that the end user's session will be kept alive based on the number of minutes entered in the text box.

In the **Inactive session lifetime (in minutes)** field, enter the number of minutes the end user's session will be kept alive.

3. Click **Apply** to open the alert box that confirms your selection.

Web-based authentication

Choose either Tier 2 or Tier 3 if Web-based authentication will be used.



NOTE: *If selecting either Tier 2 or Tier 3, please be informed that in an organization with more than 5000 users, slowness may be experienced during the authentication process. In this scenario, 8e6 recommends using an R3000 Filter with an SSL accelerator card installed. Please contact 8e6 for more information.*

Tier 2: Use time-based profiles, with time-out (in minutes) – Choose this option if using NT and/or LDAP authentication, and you want the user to have a time limit on his/her Internet connection. This option uses an authentication servlet that lets the user log into either domain with no persistent connection between the client PC and the R3000.

1. Click “Tier 2”.
2. Enter a whole number for the duration of time the user will retain his/her Internet connection.
3. Click **Apply** to open the alert box that confirms your selection.

Tier 3: Use persistent logins via a Java Applet – Choose this option if using NT and/or LDAP authentication, and you want the user to maintain a persistent network connection.

This option—the preferred method for NT authentication—opens a profile window that uses a Java applet:



Fig. 2-4 Java applet

The profile window must be kept open during the user's session in order for the user to have continued access to the Internet.



NOTE: Tier 3 Authentication requires a current version of Java Runtime Environment (JRE) on end-users' PCs. In some cases, a JRE will need to be downloaded and installed on workstations and the R3000 will allow the JRE download at the time of login. However some operating systems may require this action to be performed manually.

1. Click "Tier 3".
2. Click **Apply** to open the dialog box that informs you about the requirement of a current Java Runtime Environment (JRE) to be installed on each end user's workstation:

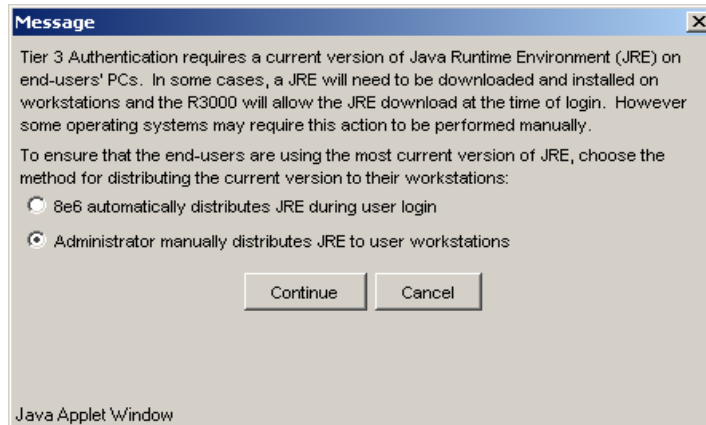


Fig. 2-5 Tier 3 dialog box

3. To ensure that end-users are using the most current version of JRE, choose the method for distributing the current version to their workstations: "8e6 automatically distributes JRE during user login" or the default selection, "Administrator manually distributes JRE to user workstations".
4. Click **Continue** to open the alert box that confirms your selection.

Enter network settings for authentication

1. Click Authentication and select Authentication Settings from the pop-up menu to display the Authentication Settings window:

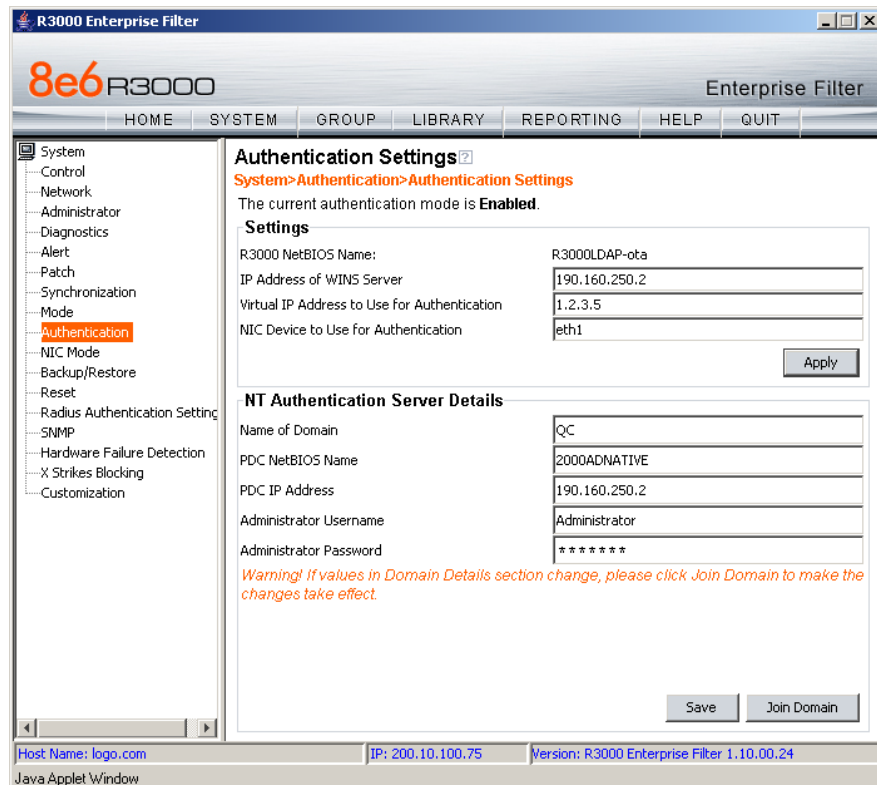


Fig. 2-6 Authentication Settings window

In the Settings frame, at the **R3000 NetBIOS Name** field the NetBIOS name of the R3000 displays. This information comes from the entry made in the Host Name field of the LAN Settings window.

2. In the **IP Address of WINS Server** field, if using a WINS server for name resolution, enter the IP address of each Windows DNS server to be filtered by this R3000, with a space between each IP address.

3. In the **Virtual IP Address to Use for Authentication** field, **1.2.3.5** displays by default. If using Tier 1 or Tier 3, enter the IP address that from now on will be used for communicating authentication information between the R3000 and the PDC. This must be an IP address that is not being used, on the same segment of the network as the R3000.



WARNING: *If the IP address entered here is not in the same subnet as this R3000, the net use connection will fail.*

4. In the **NIC Device to Use for Authentication** field:
 - if using the invisible mode, enter **eth1** (Ethernet 1) for sending traffic on the network—in particular, for transferring authentication data.
 - if using the router or firewall mode, enter **eth0** (Ethernet 0).
5. Click **Apply** to apply your settings.



NOTE: *If using the NT authentication method, you will later return to this window to join the domain. See the section on Join the NT domain in Chapter 3: NT Authentication Setup for information about these procedures.*

Create an SSL certificate

Authentication SSL Certificate should be used if Web-based authentication will be deployed on the R3000 server. Using this feature, a Secured Sockets Layer (SSL) self-signed certificate is created and placed on client machines so that the R3000 will be recognized as a valid server with which they can communicate.

Click Authentication and select Authentication SSL Certificate from the pop-up menu to display the Authentication SSL Certificate window:

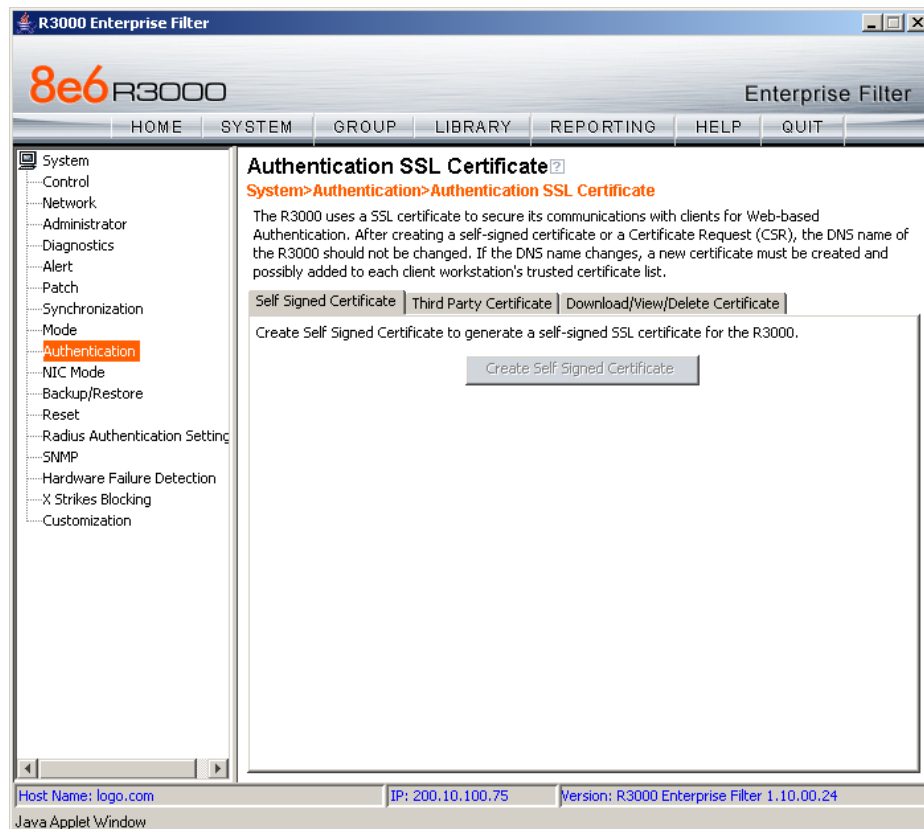


Fig. 2-7 Authentication SSL Certificate window

This window is comprised of three tabs: Self Signed Certificate, Third Party Certificate, and Download/View/Delete Certificate. These tabs are used to create, view, and/or delete self-signed or third party SSL certificates.

Create, Download a Self-Signed Certificate

1. On the Self Signed Certificate tab, click **Create Self Signed Certificate** to generate the SSL certificate.
2. Click the Download/View/Delete Certificate tab:

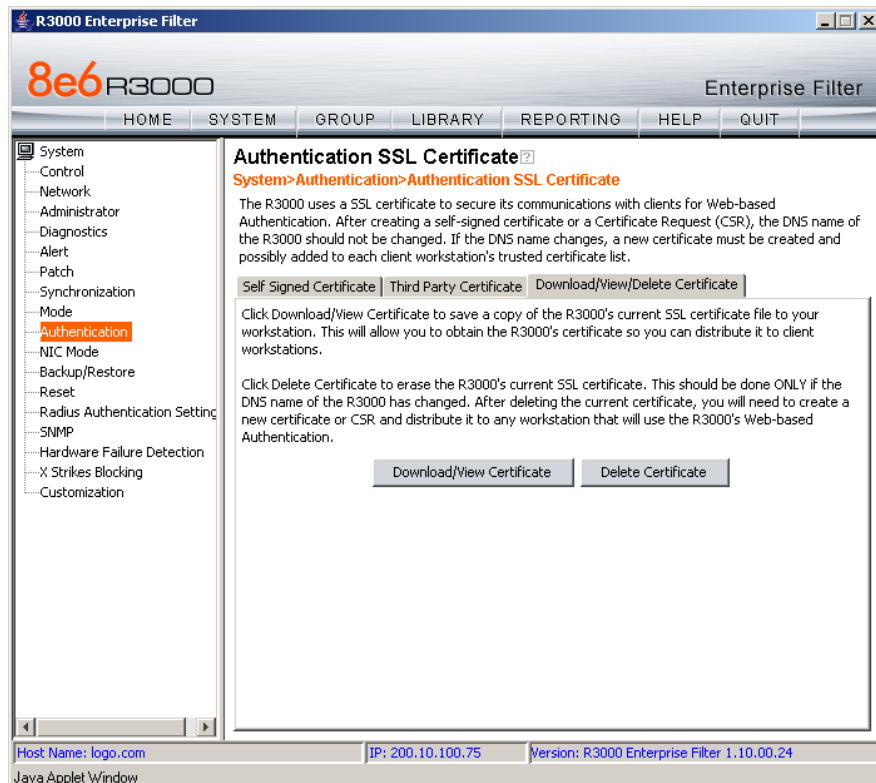


Fig. 2-8 Download/View/Delete Certificate tab

3. Click **Download/View Certificate** to open the File Download dialog box where you indicate whether you wish to Open and view the file, or open the Save As window so that you can Save the SSL certificate to a specified folder on your workstation.



NOTE: While the SSL certificate can be downloaded on a Macintosh computer, the best method to import the certificate is via the Authentication Request Form, when prompted by the Security Alert warning message to add the certificate to the trusted certificate store.

Once the certificate is saved to your workstation, it can be distributed to client workstations for users who need to be authenticated.



TIP: Click **Delete Certificate** to remove the certificate from the server.

Create, Upload a Third Party Certificate

Create a Third Party Certificate

1. Click the Third Party Certificate tab:

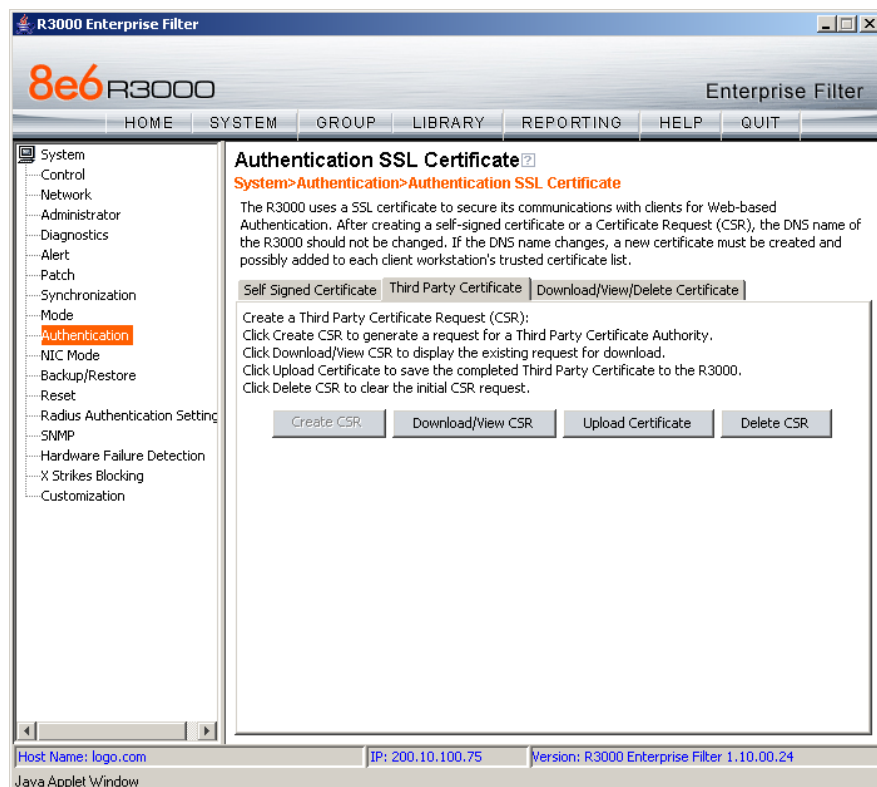


Fig. 2-9 Third Party Certificate tab



NOTE: If a third party certificate has not yet been created, the **Create CSR** button is the only button activated on this tab.

2. Click **Create CSR** to open the Create CSR pop-up window:

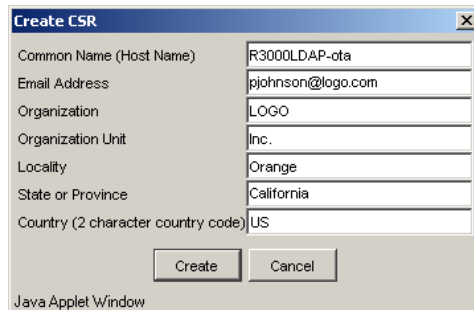


Fig. 2-10 Create CSR pop-up window

The **Common Name (Host Name)** field should automatically be populated with the host name. This field can be edited, if necessary.

3. Enter your **Email Address**.
4. Enter the name of your **Organization**, such as **8e6 Technologies**.
5. Enter an **Organizational Unit** code set up on your server, such as **Corp**.
6. Enter **Locality** information such as the name of your city or principality.
7. Enter the **State or Province** name in its entirety, such as **California**.
8. Enter the two-character **Country** code, such as **US**.
9. Click **Create** to generate the Certificate Signing Request.



NOTE: Once the third party certificate has been created, the Create CSR button displays greyed-out and the Download/View CSR, Upload Certificate, Delete CSR buttons are now activated.

Upload a Third Party Certificate

1. Click **Upload Certificate** to open the Upload Signed SSL Certificate for R3000 pop-up window:

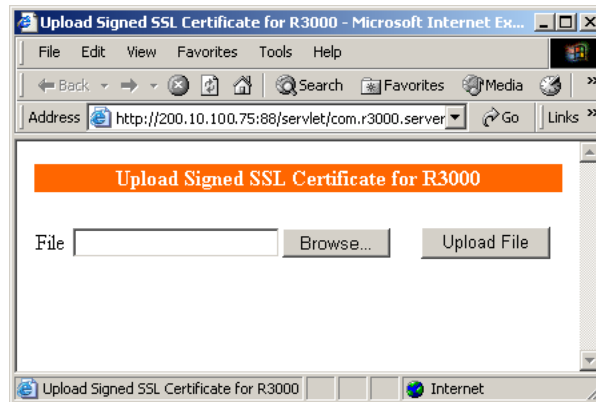


Fig. 2-11 Upload Signed SSL Certificate box

The Message dialog box also opens with the message: "Click OK when upload completes."



TIP: Click **Cancel** in the dialog box to cancel the procedure.

2. In the Upload Signed SSL Certificate for R3000 pop-up window, click **Browse** to open the Choose file window.
3. Select the file to be uploaded.
4. Click **Upload File** to upload this file to the R3000.
5. Click **OK** in the Message dialog box to confirm the upload and to close the dialog box.

Download a Third Party Certificate

1. In the Authentication SSL Certificate window, click **Download/View CSR** to open a pop-up window containing the contents of the certificate request:

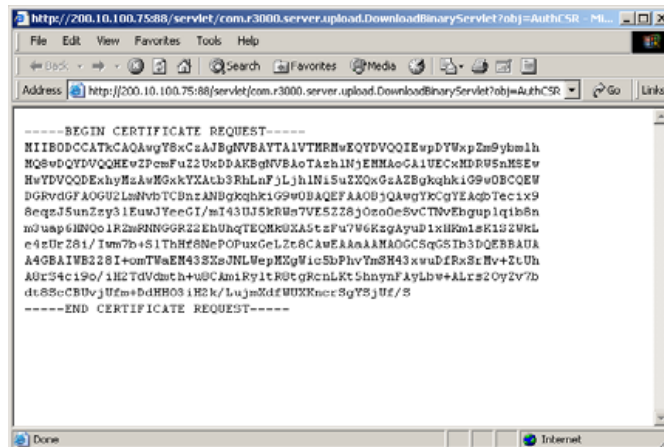


Fig. 2-12 Download CSR pop-up window

2. Click the “X” in the upper right corner of the window to close it.



TIP: Click **Delete CSR** to remove the certificate from the server.

View log results

Use the View Log File window if you need to troubleshoot any problems with the authentication setup process.

1. Click Diagnostics and select View Log File from the pop-up menu to display the View Log File window:

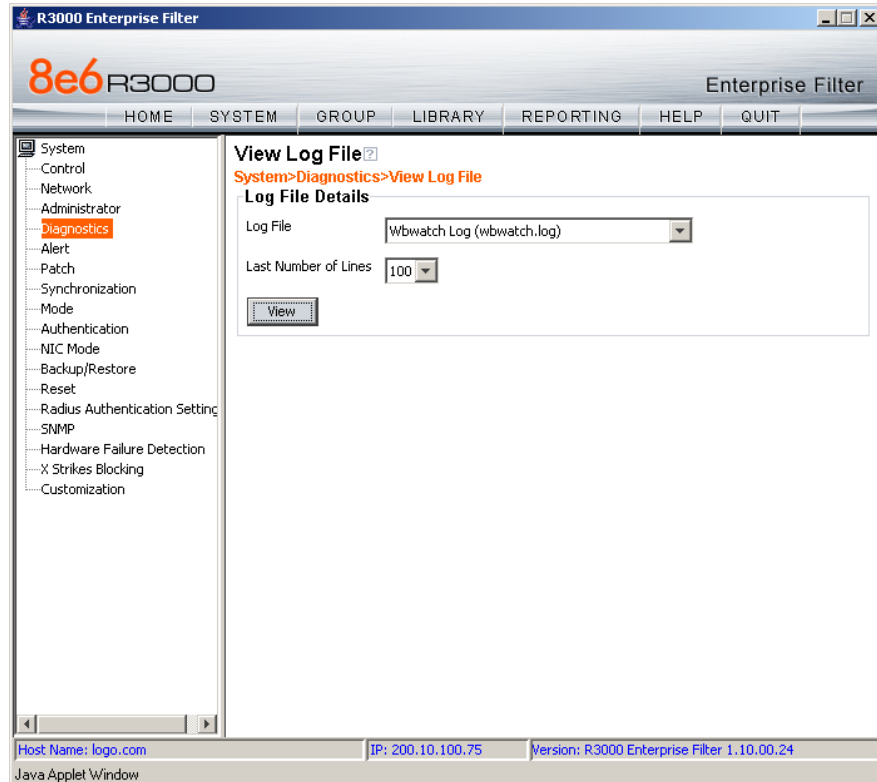


Fig. 2-13 View Log File window



NOTE: In this user guide, only authentication options will be addressed. For information about all other options, see the View Log File window in the R3000 User Guide.

2. In the Log File Details frame, select the type of **Log File** to view:
 - “User Name Log (usage.log)” - used for viewing the time and date a user logged on and off the network, along with the user's profile information.

- “Wbwatch Log (wbwatch.log)” - used for viewing messages on attempts to join the domain via the Authentication Settings window.
 - “Authentication Log (AuthenticationServer.log)” - used for viewing information about the authentication process for users, including SEVERE and WARNING error messages.
 - “Admin GUI Server Log (AdminGUIServer.log)” - used for viewing information on entries made by the administrator in the console.
 - “eDirectory Agent Debug Log (edirAgent.log)” - used for viewing the debug log, if using eDirectory LDAP authentication.
 - “eDirectory Agent Event Log (edirEvent.log)” - used for viewing the event log, if using eDirectory LDAP authentication.
 - “Authentication Module Log (authmodule.log)” - used for viewing information about SEVERE error messages pertaining to LDAP authentication connection attempts.
3. Choose the **Last Number of Lines** to view (100-500) from that file.

4. Click **View** to display results in the Result pop-up window:

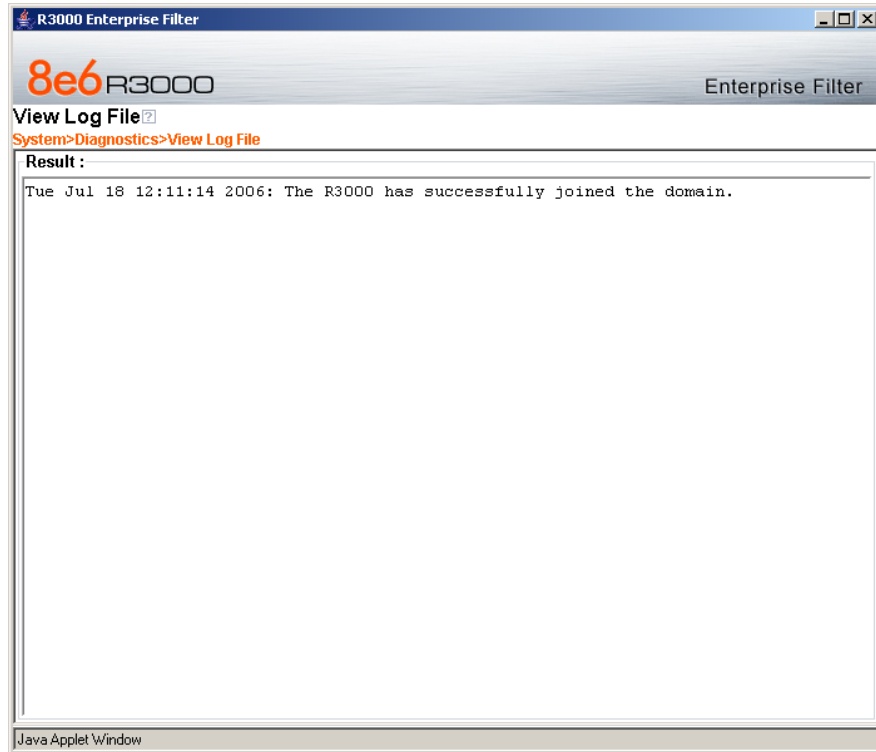


Fig. 2-14 View Log File Result pop-up window

5. Click the "X" in the upper right corner of the pop-up window to close it.

Specify block page settings

Click Control and select Block Page Authentication from the pop-up menu to display the Block Page Authentication window:

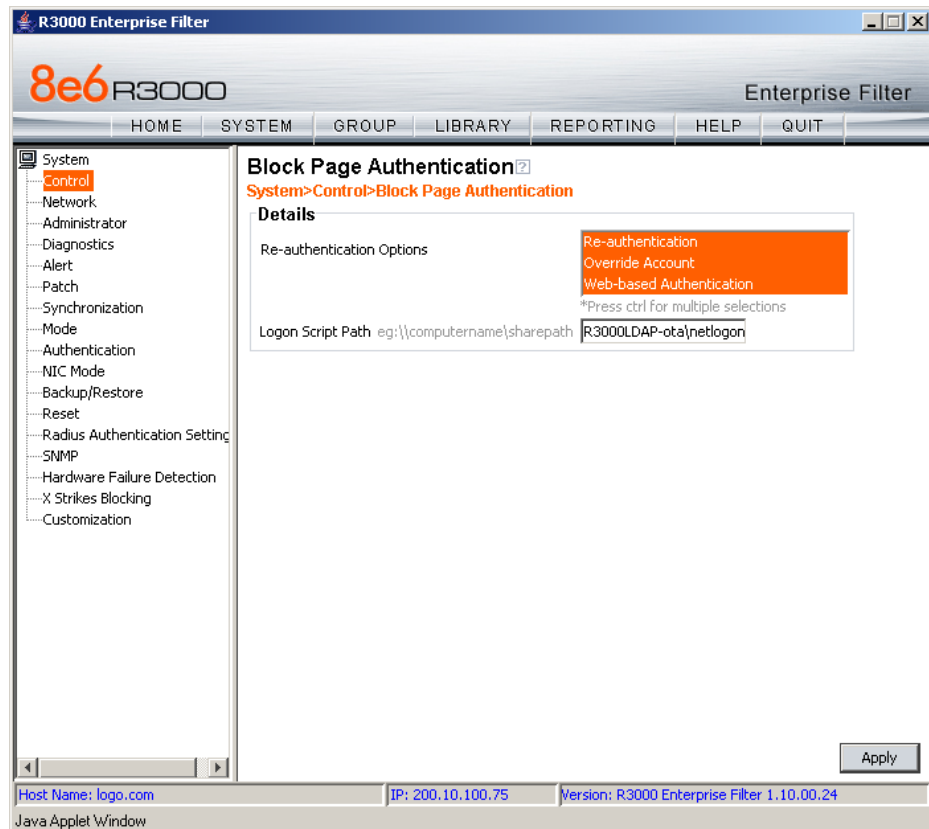


Fig. 2-15 Block Page Authentication window

Block Page Authentication

1. In the **Re-authentication Options** field of the Details frame, all block page options are selected by default, except for Web-based Authentication. Choose from the following options by clicking your selection:
 - **Web-based Authentication** - select this option if using Web authentication with time-based profiles or persistent login connections for NT or LDAP authentication methods.
 - **Re-authentication** - select this option for the re-authentication option. The user can restore his/her profile and NET USE connection by clicking an icon in a window to run a NET USE script.
 - **Override Account** - select this option if any user has an Override Account, allowing him/her to access URLs set up to be blocked at the global or IP group level.



TIP: Multiple options can be selected by clicking each option while pressing the Ctrl key on your keyboard.



NOTE: See the R3000 User Guide for information about the Override Account feature.

2. If the “Re-authentication” option was selected, in the **Logon Script Path** field, `\\PDCSHARE\scripts` displays by default. In this field, enter the path of the logon script that the R3000 will use when re-authenticating users on the network, in the event that a user's machine loses its connection with the server, or if the server is rebooted. This format requires the entry of two backslashes, the authentication server's computer name (or computer IP address) in capital letters, a backslash, and name of the share path.
3. Click **Apply** to apply your settings.

Block page

When a user attempts to access Internet content set up to be blocked, the block page displays on the user's screen:

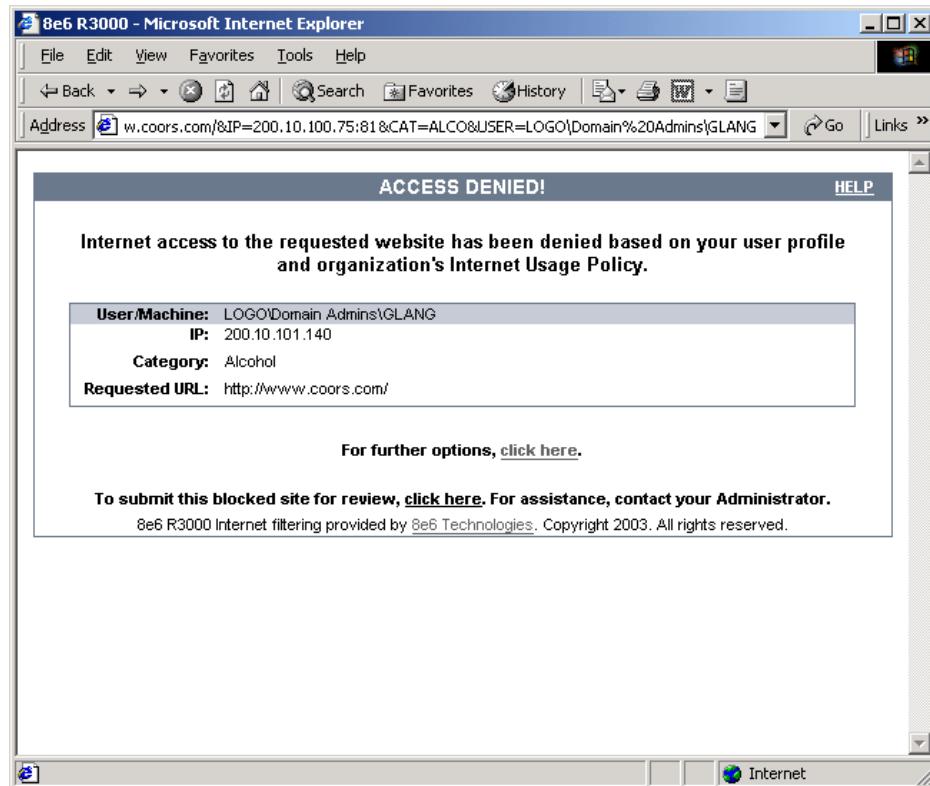


Fig. 2-16 Block page



NOTES: See *Block Page Customization* for information on adding free form text and a hyperlink at the top of the block page. Appendix D: Create a Custom Block Page from the R3000 User Guide for information on creating a customized block page using your own design.

User/Machine frame

By default, the following data displays in the User/Machine frame:

- **User/Machine** field - The username displays for the NT/LDAP user. This field is blank for the IP group user.
- **IP** field - The user's IP address displays.
- **Category** field - The name of the library category that blocked the user's access to the URL displays. If the content the user attempted to access is blocked by an Exception URL, "Exception" displays instead of the library category name.
- **Blocked URL** field - The URL the user attempted to access displays.

Standard Links

By default, the following standard links are included in the block page:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

Optional Links

By default, these links are included in the block page under the following conditions:

- **For further options, [click here](#).** - This phrase and link is included if any option was selected at the Re-authentication Options field in the Block Page Authentication window. Clicking this link takes the user to the Options window, described in the Options page sub-section that follows.
- **To submit this blocked site for review, [click here](#).** - This phrase and link is included if an email address was entered in the Submission Email Address field in the Common Customization window. Clicking this link launches the user's default email client. In the composition window, the email address from the Submission Email Address field populates the "To" field. The user's message is submitted to the global administrator.

Options page

The Options page displays when the user clicks the following link in the block page: **For further options, [click here](#).**

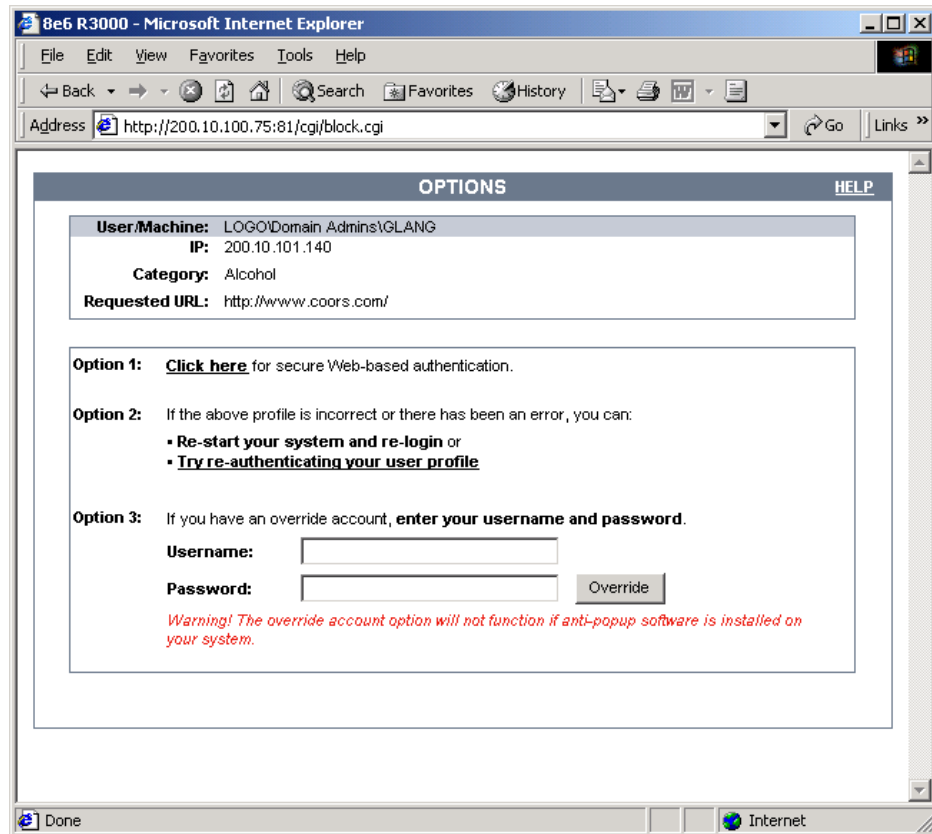


Fig. 2-17 Options page

The following items previously described for the Block page display in the upper half of the Options page:

- **BACK** and **HELP** links
- User/Machine frame contents

The frame beneath the User/Machine frame includes information for options (1, 2, and/or 3) based on settings made in the Block Page Authentication window.

Option 1

Option 1 is included in the Options page if “Web-based Authentication” was selected at the Re-authentication Options field in the Block Page Authentication window. The following phrase/link displays:

Click here for secure Web-based authentication.

When the user clicks the link, the Authentication Request Form opens:

The screenshot shows a Microsoft Internet Explorer window titled "Internet Access Authentication - Microsoft Internet Explorer". The address bar displays the URL: `https://192.168.20.10/AuthenticationServer/AuthenticationForm.jsp?URL=192.168.20.10/index.html&IP=192.168.20.000;CAT=SPORT50;USER=DEFAULT`. The main content area displays a form titled "WEB ACCESS AUTHENTICATION" with a "HELP" link. The form contains the text "Please log in to access the Internet." and an "Authentication Login" section with the following fields: Username (tjones), Password (password), Domain (Novell (LDAP)), and Alias (QC_Server). A "Log In" button is located at the bottom right of the form. At the bottom of the form, it says "8e6 R3000 Internet filtering provided by 8e6 Technologies. Copyright 2005. All rights reserved."

Fig. 2-18 Authentication Request Form



NOTE: See *Authentication Form Customization* for information on adding free form text and a hyperlink at the top of the Authentication Request Form.

Option 2

The following phrase/link displays, based on options selected at the Re-authentication Options field in the Block Page Authentication window:

- **Re-start your system and re-login** - This phrase displays for Option 1, whether or not either of the Re-authentication Options (Re-authentication, or Web-based Authentication) was selected in the Block Page Authentication window. If the user believes he/she was incorrectly blocked from a specified site or service, he/she should re-start his/her machine and log back in.
- **Try re-authenticating your user profile** - This link displays if “Re-authentication” was selected at the Re-authentication Options field, and an entry was made in the Logon Script Path field. When the user clicks this link, a window opens:

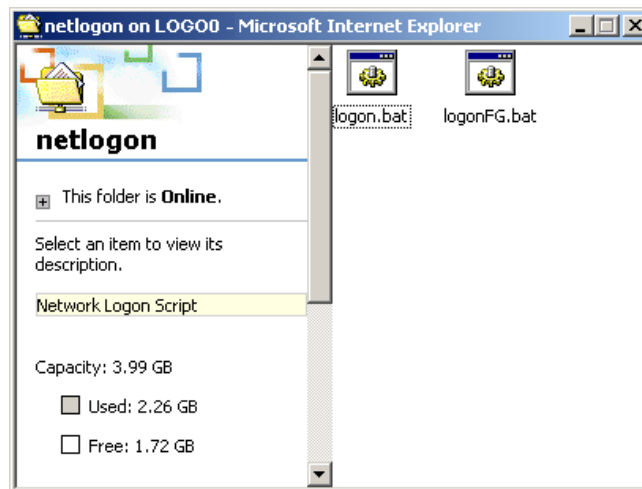


Fig. 2-19 Re-authentication option

The user should click the **logon.bat** icon to run a script that will re-authenticate his/her profile on the network.

Option 3

Option 3 is included in the Options page, if “Override Account” was selected at the Re-authentication Options field in the Block Page Authentication window.

This option is used by any user who has an override account set up for him/her by the global group administrator or the group administrator. An override account allows the user to access Internet content blocked at the global or IP sub-group level.

The user should enter his/her **Username** and **Password**, and then click **Override** to open the Profile Control window. This window must be left open throughout the user’s session in order for the user to be able to access blocked Internet content.



NOTES: See Appendix F: *Override Pop-up Blockers* for information on how a user with an override account can authenticate if a pop-up blocker is installed on his/her workstation.

See the *R3000 User Guide* for information about the *Override Account* feature.

Common Customization

Common Customization lets you specify elements to be included in block pages and/or the authentication request form end users will see.

Click Customization and then select Common Customization from the pop-up menu to display the Common Customization window:

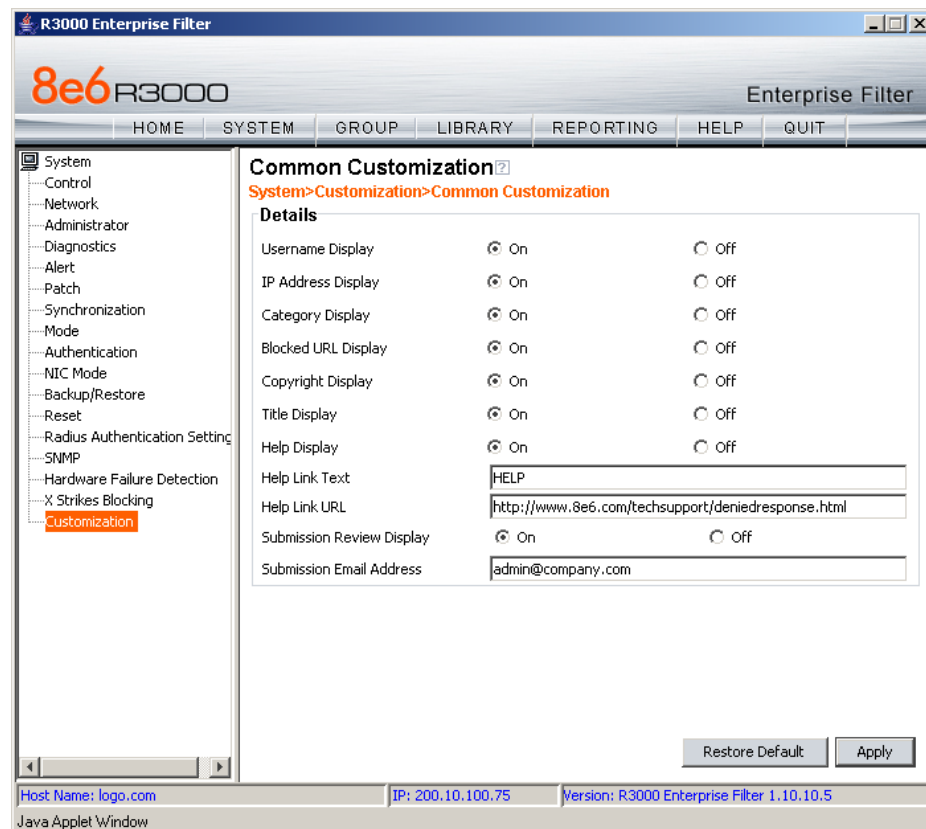


Fig. 2-20 Common Customization window

By default, in the Details frame all elements are selected to display in the HTML pages, the Help link points to the FAQs page on 8e6's public site that explains why access was denied, and a sample email address is included for administrator contact information. These details can be modified, as necessary.

Enable, Disable Features

1. Click “On” or “Off” to enable or disable the following elements in the HTML pages, and make entries in fields to display customized text, if necessary:
 - Username Display - if enabled, displays “User/ Machine” followed by the end user’s username in block pages
 - IP Address Display - if enabled, displays “IP” followed by the end user’s IP address in block pages
 - Category Display - if enabled, displays “Category” followed by the long name of the blocked category in block pages
 - Blocked URL Display - if enabled, displays “Blocked URL” followed by the blocked URL in block pages
 - Copyright Display - if enabled, displays 8e6 R3000 copyright information at the footer of block pages and the authentication request form
 - Title Display - if enabled, displays the title of the page in the title bar of the block pages and the authentication request form
 - Help Display - if enabled, displays the specified help link text in block pages and the authentication request form. The associated URL (specified in the Help Link URL field described below) is accessible to the end user by clicking the help link.



NOTE: *If enabling the Help Display feature, both the Help Link Text and Help Link URL fields must be populated.*

- **Help Link Text** - By default, *HELP* displays as the help link text. Enter the text to display for the help link.

- **Help Link URL** - By default, *http://www.8e6.com/tech-support/deniedresponse.html* displays as the help link URL. Enter the URL to be used when the end user clicks the help link text (specified in the Help Link Text field).
- **Submission Review Display** - if enabled, displays in block pages the email address of the administrator to receive requests for a review on sites the end users feel are incorrectly blocked. The associated email address (specified in the Submission Email Address field described below) is accessible to the end user by clicking the **click here** link.



NOTE: *If enabling the Submission Review Display feature, an email address entry of the designated administrator in your organization must be made in the Submission Email Address field.*

- **Submission Email Address** - By default, *admin@company.com* displays in block pages as the email address of the administrator to receive feedback on content the end user feels has been incorrectly blocked. Enter the global administrator's email address.

2. Click **Apply** to save your entries.



TIP: *Click **Restore Default** to revert to the default settings.*

Authentication Form Customization

To customize the Authentication Request Form, click Customization and select Authentication Form from the pop-up menu:

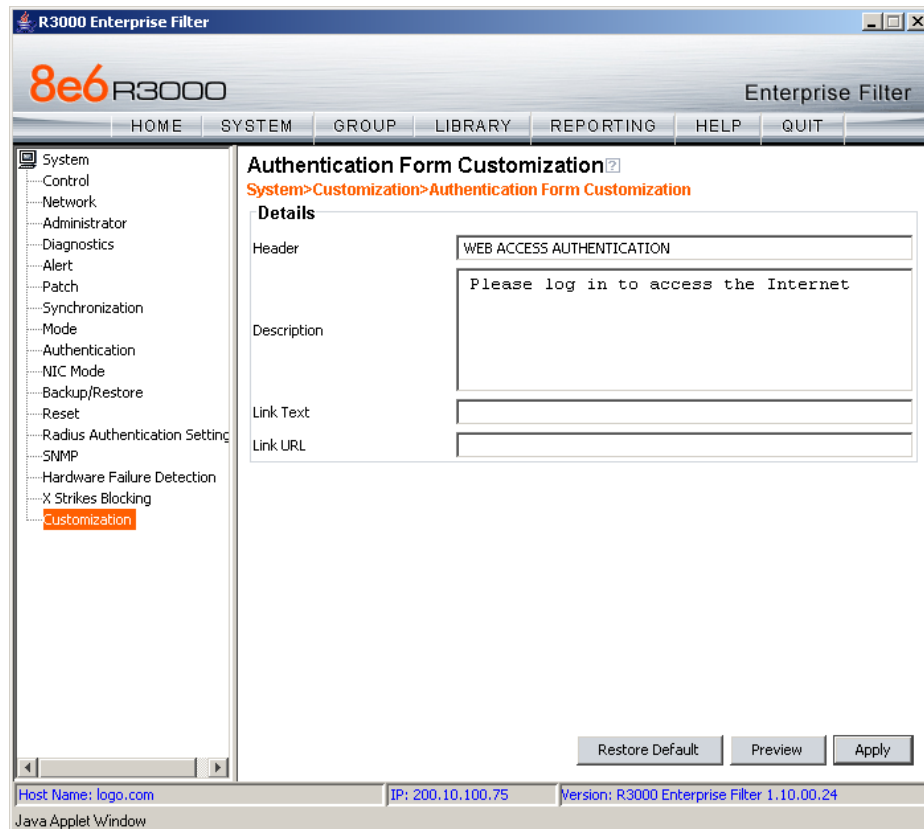


Fig. 2-21 Authentication Form Customization window

 **NOTE:** This window is activated only if Authentication is enabled via System > Authentication > Enable/Disable Authentication, and Web-based Authentication is specified.

 **TIP:** An entry in any of the fields in this window is optional, but if an entry is made in the Link Text field, a corresponding entry must also be made in the Link URL field.

1. Make an entry in any of the following fields:

- In the **Header** field, enter a static header to be displayed at the top of the Authentication Request Form.
- In the **Description** field, enter a static text message to be displayed beneath the Authentication Request Form header.
- In the **Link Text** field, enter text for the link's URL to be displayed beneath the Description in the Authentication Request Form, and in the **Link URL** field, enter the corresponding hyperlink in plain text using the *http://* or *https://* syntax.

Any entries made in these fields will display centered in the Authentication Request Form, using the Arial font type.

2. Click **Apply**.



TIP: Click **Restore Default** to revert to the default text in this window.

Preview Sample Authentication Request Form

1. Click **Preview** to launch a separate browser window containing a sample Authentication Request Form, based on entries saved in this window and in the Common Customization window:

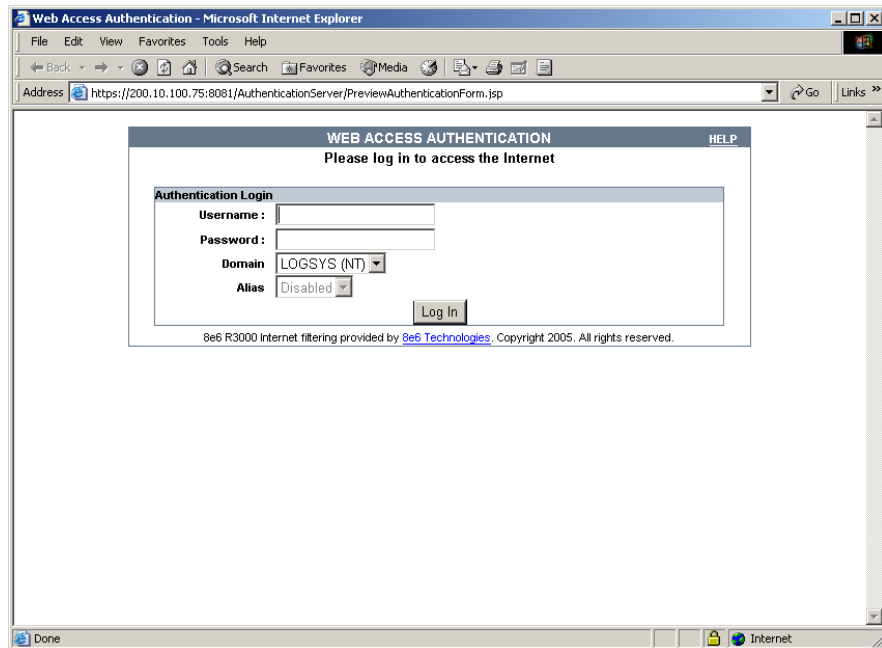


Fig. 2-22 Sample Customized Authentication Request Form

By default, the following data displays in the frame:

- **Username** field - The username displays.
- **Password** field - The user's IP address displays.
- **Domain** field - All LDAP domain names set up on the R3000 display in the pull-down menu.
- **Alias** field (optional) - All alias names associated with the LDAP domain specified in the field above display in the pull-down menu, if the account names were entered for that LDAP domain.

By default, the following standard links are included in the Authentication Request Form:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

2. Click the "X" in the upper right corner of the window to close the sample Authentication Request Form.



TIP: *If necessary, make edits in the Authentication Form Customization window or the Common Customization window, and then click **Preview** in this window again to view a sample Authentication Request Form.*

Block Page Customization

To customize the block page, click Customization and select Block Page from the pop-up menu:

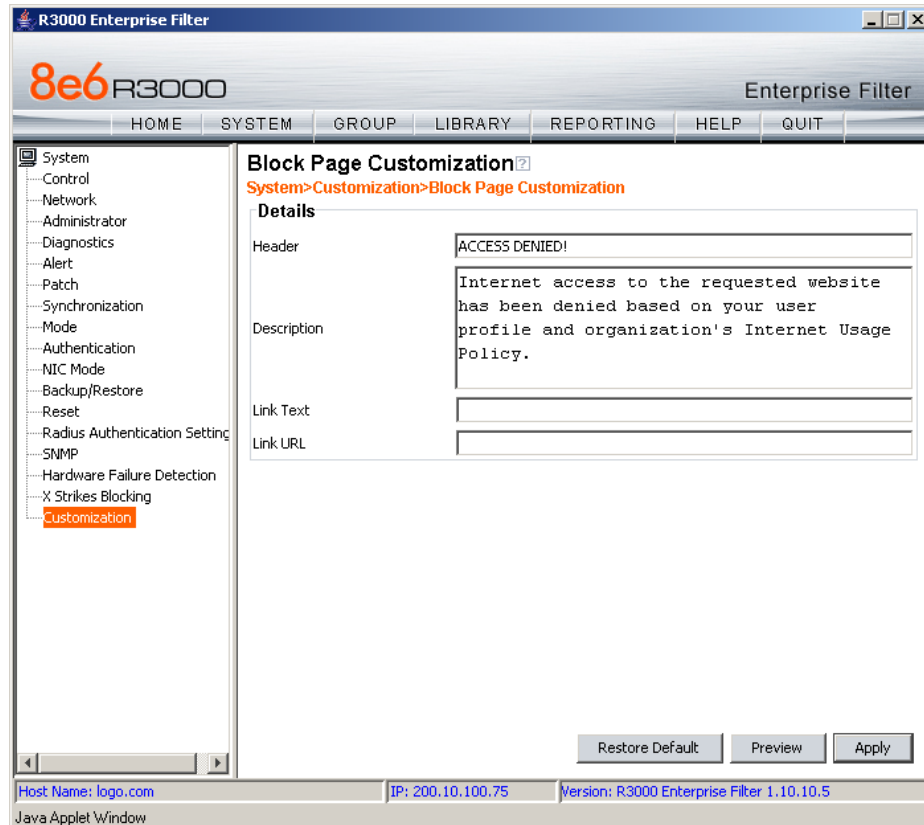


Fig. 2-23 Block Page Customization window



NOTE: See Appendix D: Create a Custom Block Page from the R3000 User Guide for information on creating a customized block page using your own design.



TIP: An entry in any of the fields in this window is optional, but if an entry is made in the Link Text field, a corresponding entry must also be made in the Link URL field.

1. Make an entry in any of the following fields:

- In the **Header** field, enter a static header to be displayed at the top of the block page.
- In the **Description** field, enter a static text message to be displayed beneath the block page header.
- In the **Link Text** field, enter text for the link's URL to be displayed beneath the Description in the block page, and in the **Link URL** field, enter the corresponding hyperlink in plain text using the *http://* or *https://* syntax.

Any entries made in these fields will display centered in the customized block page, using the Arial font type.

2. Click **Apply**.



TIP: Click **Restore Default** to revert to the default text in this window.

Preview Sample Block Page

1. Click **Preview** to launch a separate browser window containing a sample customized block page, based on entries saved in this window and in the Common Customization window:

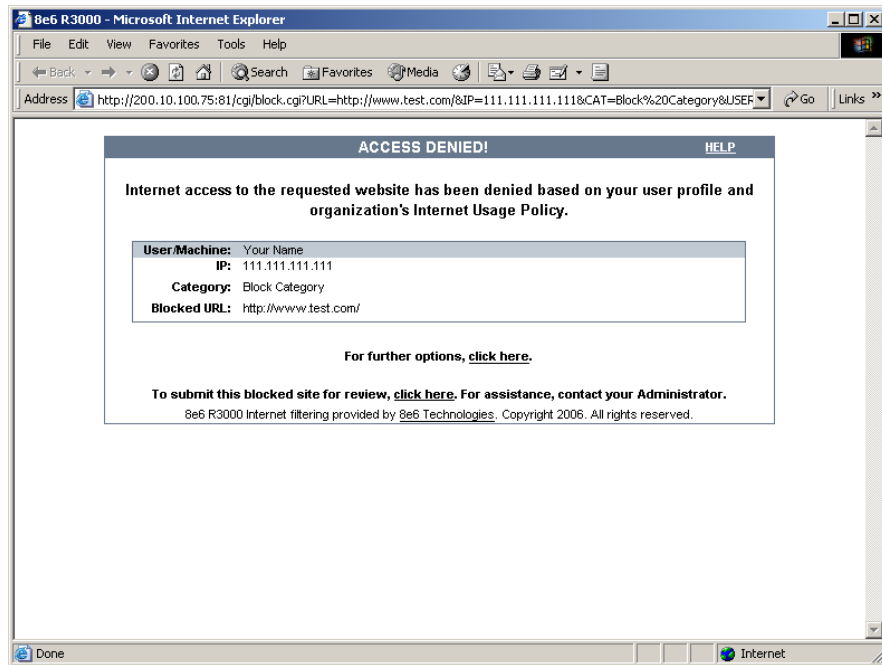


Fig. 2-24 Sample Customized Block Page

By default, the following data displays in the User/Machine frame:

- **User/Machine** field - The username displays for the NT/LDAP user. This field is blank for the IP group user.
- **IP** field - The user's IP address displays.
- **Category** field - The name of the library category that blocked the user's access to the URL displays. If the content the user attempted to access is blocked by an Exception URL, "Exception" displays instead of the library category name.
- **Blocked URL** field - The URL the user attempted to access displays.

By default, the following standard links are included in the block page:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

By default, these links are included in the block page under the following conditions:

- **For further options, [click here](#).** - This phrase and link is included if any option was selected at the Re-authentication Options field in the Block Page Authentication window. Clicking this link takes the user to the Options window, described in the Options page subsection.
 - **To submit this blocked site for review, [click here](#).** - This phrase and link is included if an email address was entered in the Submission Email Address field in the Common Customization window. Clicking this link launches the user's default email client. In the composition window, the email address from the Submission Email Address field populates the "To" field. The user's message is submitted to the global administrator.
2. Click the "X" in the upper right corner of the window to close the sample customized block page.



TIP: If necessary, make edits in the Block Page Customization window or the Common Customization window, and then click **Preview** in this window again to view a sample block page.

CHAPTER 3: NT AUTHENTICATION SETUP



NOTE: If you are running a Windows 2000 or Windows 2003 Server and are using the NTLM authentication protocol, then you need to make SMB Signing “not required.” See Appendix D: Disable SMB Signing Requirements for steps on how to disable SMB Signing restrictions.

Join the NT Domain

Click Authentication and select Authentication Settings from the pop-up menu to display the Authentication Settings window:

R3000 Enterprise Filter

8e6 R3000 Enterprise Filter

HOME SYSTEM GROUP LIBRARY REPORTING HELP QUIT

System
Control
Network
Administrator
Diagnostics
Alert
Patch
Synchronization
Mode
Authentication
NIC Mode
Backup/Restore
Reset
Radius Authentication Setting
SNMP
Hardware Failure Detection
X Strikes Blocking
Customization

Authentication Settings
System>Authentication>Authentication Settings
The current authentication mode is **Enabled**.

Settings

R3000 NetBIOS Name: R3000LDAP-ota
IP Address of WINS Server: 190.160.250.2
Virtual IP Address to Use for Authentication: 1.2.3.5
NIC Device to Use for Authentication: eth1

Apply

NT Authentication Server Details

Name of Domain: QC
PDC NetBIOS Name: 2000ADNATIVE
PDC IP Address: 190.160.250.2
Administrator Username: Administrator
Administrator Password: *****

Warning! If values in Domain Details section change, please click Join Domain to make the changes take effect.

Save Join Domain

Host Name: logo.com IP: 200.10.100.75 Version: R3000 Enterprise Filter 1.10.00.24
Java Applet Window

Fig. 3-1 Authentication Settings window

Information should only be entered in the NT Authentication Server Details frame if the R3000 will use the NT Authentication method to authenticate users.



NOTE: The following Windows servers are supported by the current version of authentication: NT 4.0 SP4 or later, Mixed Mode 2000, and 2003. A Windows 2003 server may require changes to the default settings for SMB signing to allow communications.

The account that is provided for accessing the Windows server must have the administrative rights to add a machine account to the specified domain on the R3000. This requirement ensures the R3000 will be able to authenticate users from the Windows domain.

1. Enter the alphanumeric **Name of Domain** on which this server resides, using capital letters.
2. Using capital letters, enter up to 15 alphanumeric characters of the **PDC NetBIOS Name**, which is the computer name of the authentication server, or Primary Domain Controller.
3. Enter the **PDC IP Address**, which is the authentication server's IP address.
4. Enter the **Administrator Username** and **Administrator Password**. This account used for joining the domain must have administrator privileges.
5. Click **Join Domain** to save your entries and to submit a request for the R3000 to join the domain.



TIP: If entries in the NT Authentication Server Details frame are modified after joining the domain, you must join the domain again.



NOTE: Click **Save** if you are only pre-configuring the box. This option lets you save credentials without re-entering the information each time the domain is joined, or if the R3000 gets out of sync with the Primary Domain Controller.

Create an NT Domain

After joining the domain, go to the Group section of the console and add an NT domain that contains entities to be authenticated.

Add an NT domain

1. Click NT in the control panel to open the pop-up menu, and select Add Domain to open the Create Domain Controller dialog box:

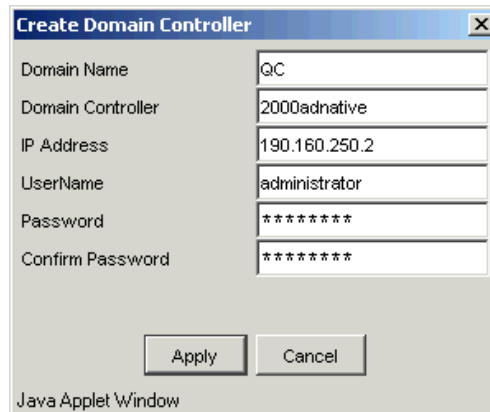


Fig. 3-2 Create Domain Controller

2. In the **Domain Name** field, enter the name of the domain on which the R3000 resides, using capital letters.



NOTE: The Domain Name must be the same name entered in the Authentication Settings window's Name of Domain field.

3. In the **Domain Controller** field, enter the name of the authentication server for the domain.
4. Enter the domain controller's **IP Address**.
5. In the **UserName** field, enter the username of the administrator.
6. Enter the password in the **Password** and **Confirm Password** fields.

7. Click **Apply** to add the domain to the tree.

Refresh the NT branch

Click NT in the control panel to open the pop-up menu, and select **Refresh** whenever changes have been made in this branch of the tree.

View or modify NT domain details

Domain Settings

1. Double-click NT in the control panel to open the NT branch of the Group tree. Select the NT domain you added, and choose Domain Details from the pop-up menu to display the default Settings tab of the NT Domain Details window:

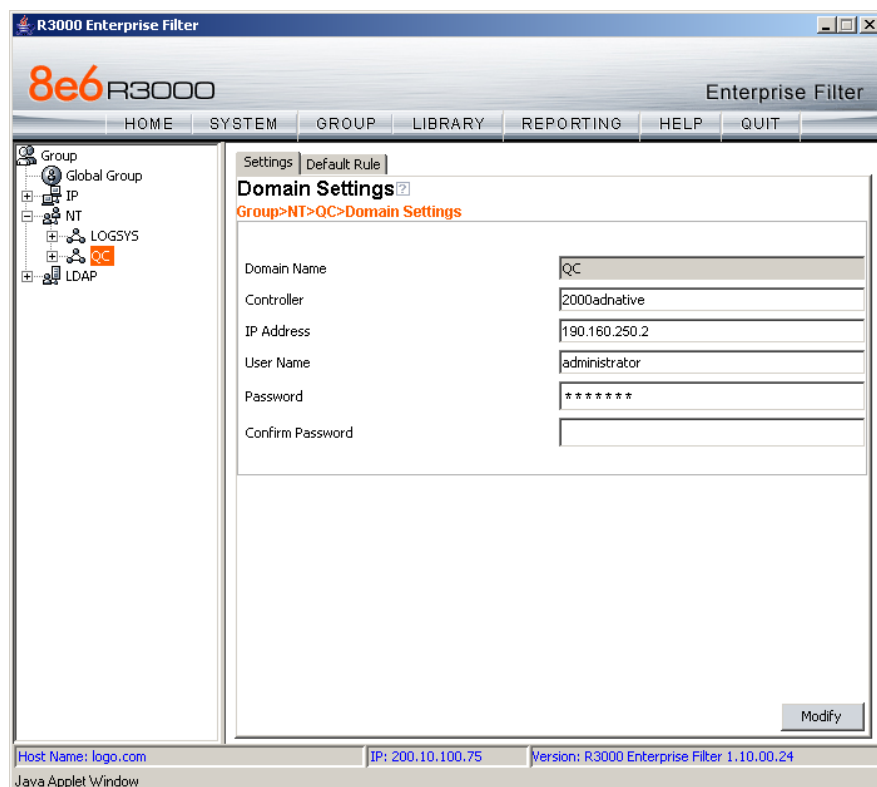


Fig. 3-3 NT Domain Details window, Settings tab



NOTE: To enter profile information for NT groups and users once domain settings are established, see *Set up NT Domain Groups, Members*.

2. For the Domain Settings:

- The **Domain Name** entered in the Create Domain Controller dialog box displays greyed-out and cannot be modified.
- The following fields can be modified: name of the domain **Controller**, **IP Address**, **User Name**, **Password**, and **Confirm Password**.

Whenever criteria on this tab is modified:

- a. The password from the Password field must be entered in the **Confirm Password** field for verification.
- b. Click **Modify** to apply your settings.

Default Rule

1. Click the Default Rule tab to display the Default Rule settings of the NT Domain Details window:

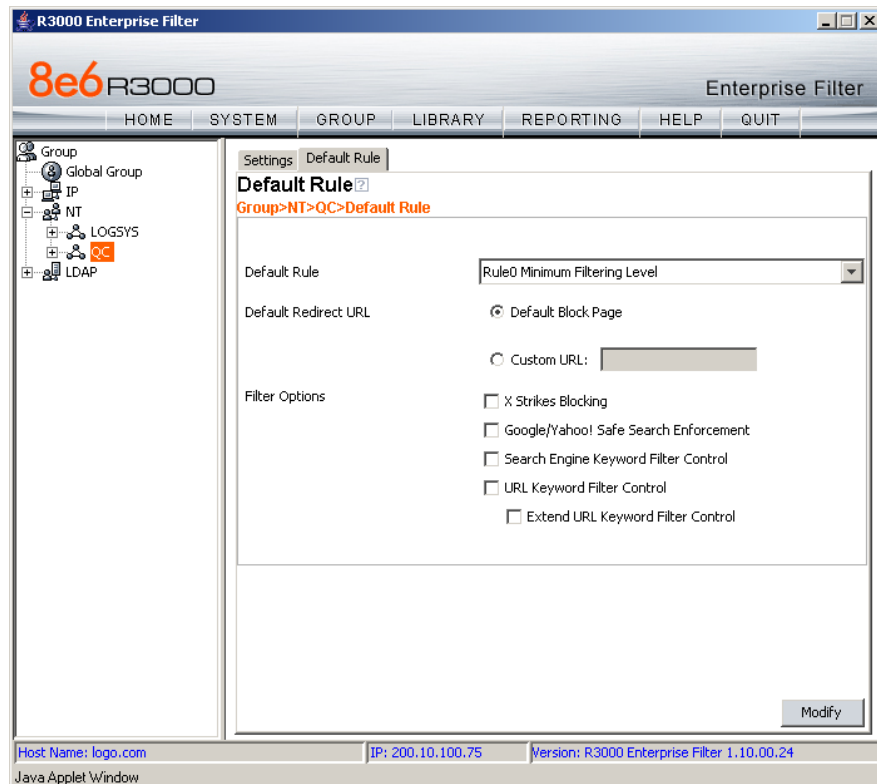


Fig. 3-4 NT Domain Details window, Default Rule tab

2. For the Default Rule:
 - “Rule0, the Minimum Filtering Level” displays by default as the **Default Rule**. If this rule is used, it will be applied to all groups and members in the NT domain without a filtering profile established.
 - “Default Block Page” is selected by default as the **Default Redirect URL**. If the default block page is used, it will be applied to all groups and members in the NT domain without a filtering profile established. If “Custom URL” is selected, a URL must be entered in the corresponding text box.

- **Filter Options** that have been selected display check marks in corresponding checkboxes for “X Strikes Blocking”, “Google/Yahoo! Safe Search Enforcement”, “Search Engine Keyword Filter Control”, “URL Keyword Filter Control”, and “Extend URL Keyword Filter Control”.

Whenever criteria on this tab is modified, click **Modify** to apply your settings.

Delete an NT domain

To delete a domain profile, choose Delete from the NT domain menu. This action removes the domain from the tree.

Set up NT Domain Groups, Members

In the control panel, the NT domain branch of the tree menu includes options for setting up groups and/or members in the domain so that filtering profiles can later be created. The following options are used in this setup process: Select Group/Member from Domain, Set Group Priority, Manually Add Member, Manually Add Group, and Upload User/Group Profile.

Add NT groups, members to the tree

Before you can create filtering profiles for groups and/or members in a domain, you must first add the groups and/or members to the tree list for that domain.

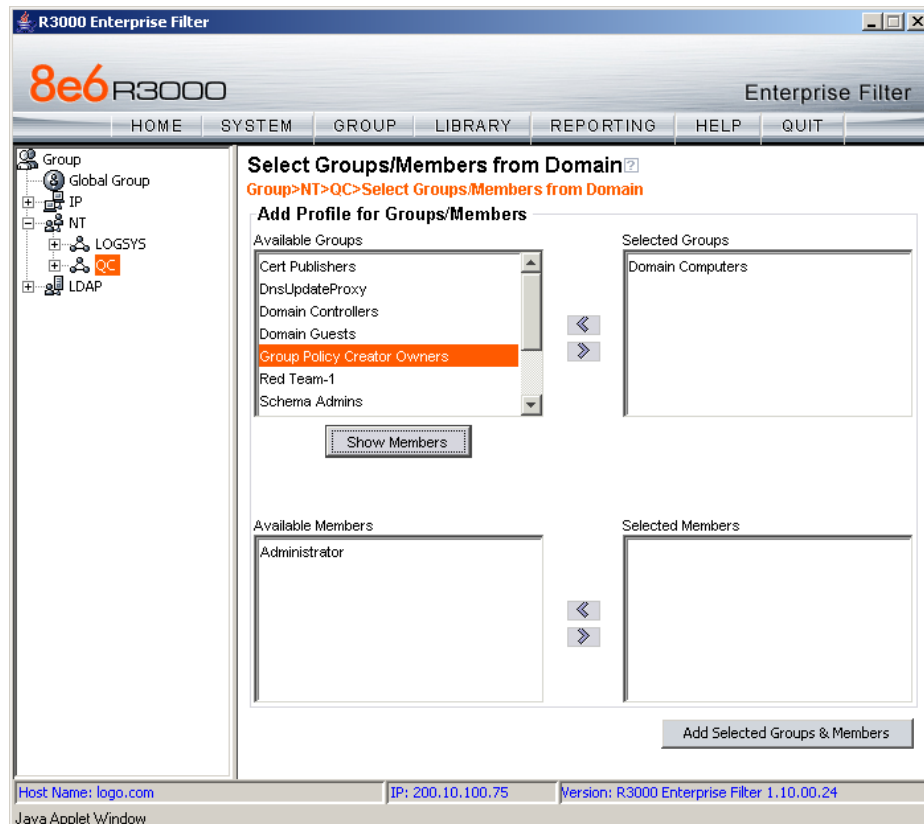


Fig. 3-5 Select Groups/Members from Domain window

Select the NT domain, and choose Select Group/Member from Domain from the pop-up menu to display the Select Groups/Members from Domain window (see Figure 3-5).

To add groups—that need filtering profiles—to the tree list:

1. Choose a group from the Available Groups list box.
2. Use the right arrow button (>) to move the group to the Selected Groups list box.

If necessary, select a group and use the left arrow button (<) to move the group back to the Available Groups list box.

To add group members—who need filtering profiles—to the tree list:

1. Choose the group from the Available Groups list box.
2. Click **Show Members** to display group members in the Available Members list box.
3. Choose a member from the Available Members list box, and use the right arrow button (>) to move the group to the Selected Members list box.

If necessary, select a member and use the left arrow button (<) to move the member back to the Available Members list box.

When all entities who need filtering profiles have been added to the selected Groups and/or Selected Members list box(es), click **Add Selected Groups & Members** to add them within the domain's section of the tree list.



NOTE: See *Add or maintain an entity's profile under Create and Maintain NT Profiles* for information on defining the filtering profile for the group.



WARNING: When adding an NT group or member to the tree list, the group/member will be blocked from Internet access if the minimum filtering level has not been defined via the Minimum Filtering Level window. If you have just established the minimum filtering level, filter settings will not be effective until the group member/user logs off and back on the server. Refer to the R3000 User Guide for more information on the minimum filtering level.

Specify a group's filtering profile priority

1. Select the NT domain, and choose Set Group Priority from the pop-up menu to display the Set Group Priority window:

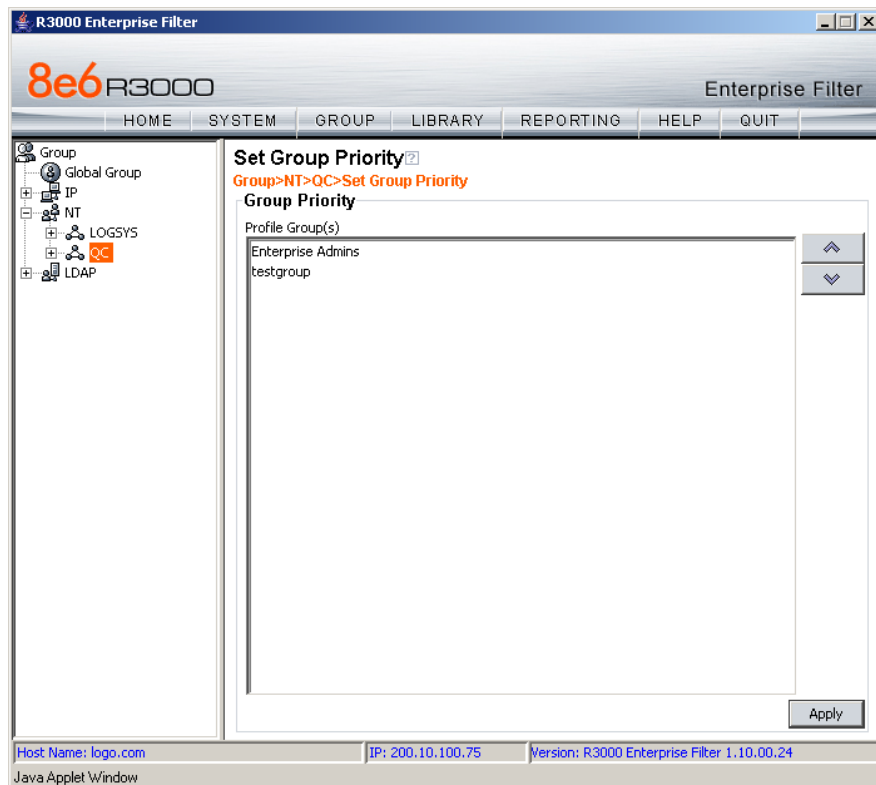


Fig. 3-6 Set Group Priority window

This window is used for designating which group profile will be assigned to a user when he/she logs in. If a user is a member of multiple groups, the one that is positioned highest in the list is applied.



NOTES: Groups automatically populate the Profile Group(s) list box, if these groups have one or more identical users and were added to the tree list via the Select Groups/Members from Domain window.

An entry for the Group Priority list is added to the end of the list when the group profile for that group is added to the R3000, and is removed automatically when you delete the profile.

2. To change the filtering priority of groups:
 - a. Select a group from the Profile Group(s) list box.
 - b. Use the up or down arrow button to move that group up or down in the list.
 - c. Click **Apply** to apply your settings.

Manually add a user's name to the tree

1. Select the NT domain, and choose Manually Add Member from the pop-up menu to open the Manually Add Member dialog box:

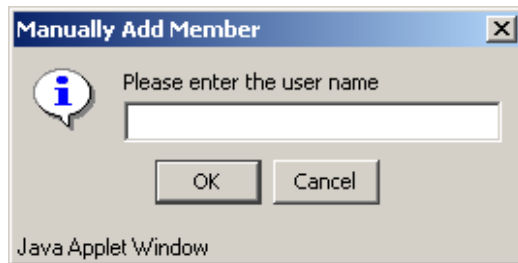


Fig. 3-7 Manually Add Member box

This dialog box is used for adding a username to the tree list, so that a filtering profile can be defined for that user.

2. Enter the username in the text box, up to 16 characters.



TIP: NT usernames should be entered without breaks or spaces. The first character must be a letter. The following ASCII characters can be used: "A-Z", "a-z", "0-9", "_" (underscore), and "-" (hyphen).

Examples:

TJONES

JSmith

Jane_Doe

Doe-John

3. Click **OK** to add the username to the domain's section of the tree.



NOTE: See *Add or maintain an entity's profile under Create and Maintain NT Profiles* for information on defining the filtering profile for the user.

Manually add a group's name to the tree

1. Select the NT domain, and choose Manually Add Group from the pop-up menu to open the Manually Add Group dialog box:

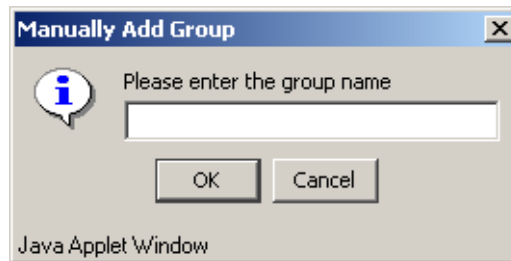


Fig. 3-8 Manually Add Group box

This dialog box is used for adding a group name to the tree list, so that a filtering profile can be defined for that group.

2. Enter the group's name in the text box.
3. Click **OK** to add the group name to the domain's section of the tree.



NOTE: See *Add or maintain an entity's profile under Create and Maintain NT Profiles* for information on defining the filtering profile for the group.

Upload a file of filtering profiles to the tree

1. Select the NT domain, and choose Upload User/Group Profile from the pop-up menu to display the Upload User/Group Profile window:

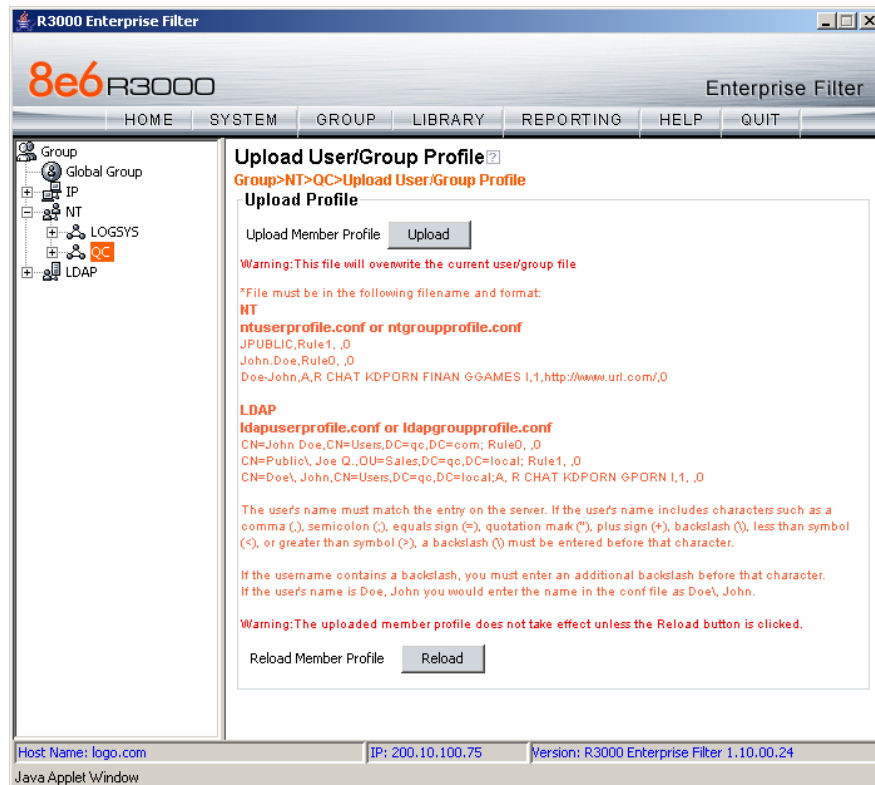


Fig. 3-9 Upload User/Group Profile window

This window is used for uploading a file to the tree with user or group names and their associated filtering profiles.

2. Click **Upload** to open the Upload Member Profile File pop-up window:

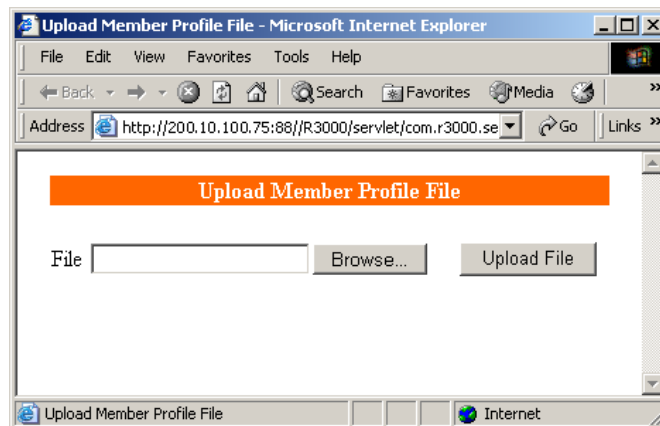


Fig. 3-10 Upload Member Profile File window

3. Click **Browse** to open the Choose file window.
4. Select the file to be uploaded.

 **WARNING:** Any file uploaded to the server will overwrite the existing user/group profile file.

Each user/group profile in the file uploaded to the server **must be** set up in a specified format in order for the profile to be activated on the server. This format differs depending on whether the profiles are user or group profiles. Based on the type of file format used, the file should have the following name:

- **ntuserprofile.conf** if the file contains NT user profiles
- **ntgroupprofile.conf** if the file contains NT group profiles

 **NOTE:** See Appendix A: User/Group File Format and Rules for examples of valid filtering profile formats to use when creating a list of profiles to be uploaded to the server.

 **WARNING:** When uploading a list of profiles to the tree list, the user will be blocked from Internet access if the minimum filtering level has not been defined via the Minimum Filtering Level window. If you have just established the minimum filtering level, filter settings will not be effective until the user logs off and back on the server. Refer to the R3000 User Guide for more information on the minimum filtering level.

5. Click **Upload File** to upload this file to the server. The Upload Successful pop-up window informs you to click Reload in order for these changes to be effective.
6. Click **Reload**.
7. Go to the NT branch of the tree, and choose **Refresh** from the NT group menu.

Create and Maintain NT Profiles

Once an NT group or member has been added to the tree, a filtering profile can be created and maintained for that entity. For groups, the following options are available for filtering profile creation and maintenance: Group Member Details, Profile, and Remove. For members, the following options are available for filtering profile creation and maintenance: Profile, and Remove.

Add an NT group, member to the tree list

Select the NT domain, and choose Group Member Details from the pop-up menu to display the Group/Member Details window:

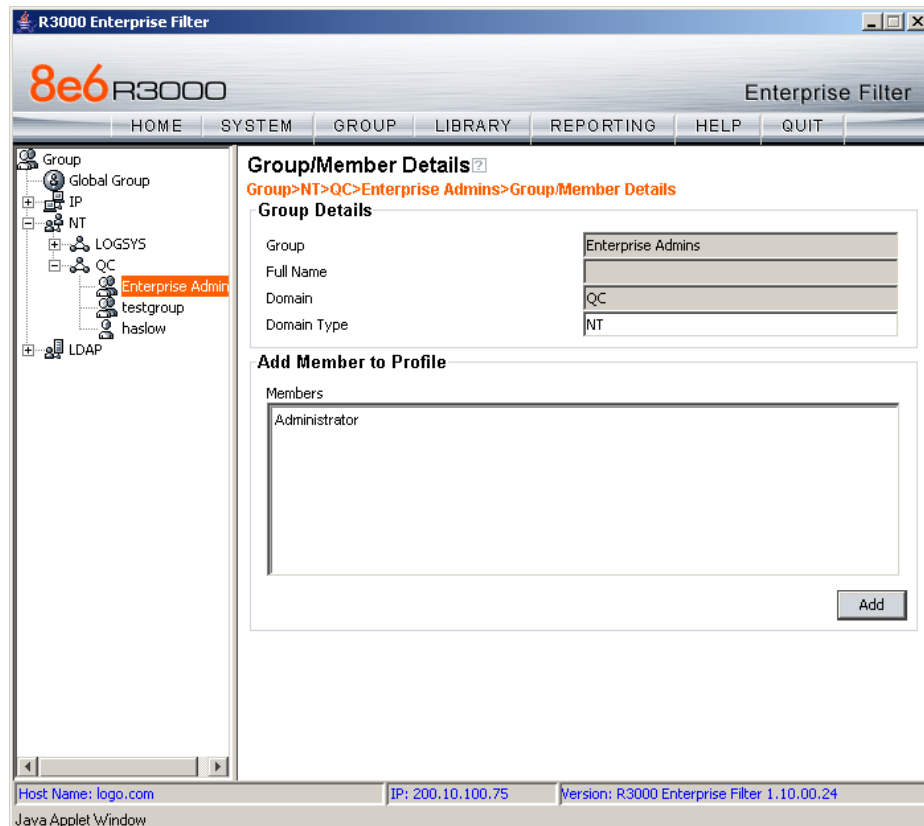


Fig. 3-11 Group/Member Details window

This window is used for viewing profile information about a group, and for adding members to a group.

In the Group Details frame, the following details display: **Group** name, **Domain** name, and **Domain Type**. Members that belong to the group display in the Members list box in the Add Member to Profile frame.

To add a member to the tree list so that a profile can be created for that member:

1. Select the entity from the Members list box.
2. Click **Add**.

Add or maintain an entity's profile

Select the NT domain, and choose Profile from the pop-up menu to display the default Category tab of the Profile window:

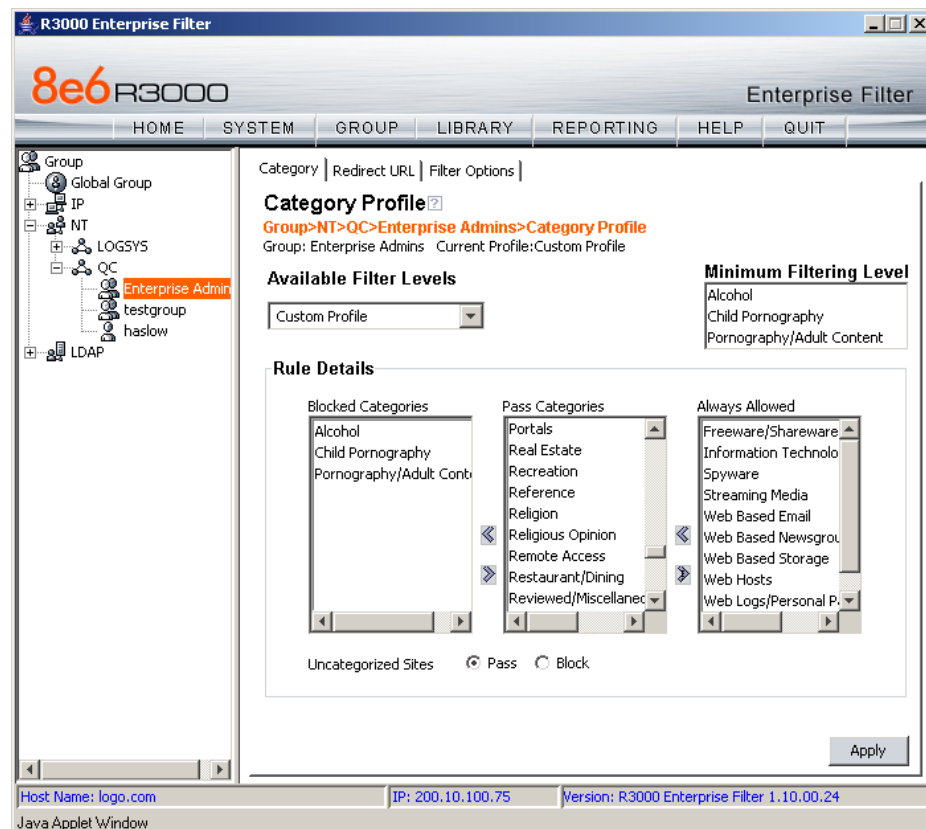


Fig. 3-12 Group Profile window, Category tab

The Profile window is used for viewing/creating the filtering profile of the defined entity (group or member). Entries made in the Category, Redirect URL, and Filter Options tabs comprise the profile string for the entity.

Category Profile

Category Profile is used for creating the categories portion of the filtering profile for the entity.



NOTE: *In order to use this tab, filtering rules should already have been set up via the Rules window, accessible from the Global Group options, and the minimum filtering level should already be established. The minimum filtering level is set up in the Minimum Filtering Level window, accessible from the Global Group options. See the R3000 User Guide for more information about these windows.*

By default, “Rule0 Minimum Filtering Level” displays in the **Available Filter Levels** pull-down menu, and the Minimum Filtering Level box displays “Child Pornography” and Pornography/Adult Content”. By default, **Uncategorized Sites** are allowed to Pass.



NOTE: *By default, the **Available Filter Levels** pull-down menu also includes these three rule choices: Rule1 BYPASS”, “Rule2 BLOCK Porn”, “Rule3 Block IM and Porn”, and “Rule4 8e6 CIPA Compliance”.*

To create the category portion of the entity’s filtering profile:

1. Select a filtering rule from the available choices:
 - If you select a filtering rule from the **Available Filter Levels** pull-down menu, this action automatically populates the Blocked Categories, Pass Categories, and/or Always Allowed list box(es) in the Rule Details frame with library categories set up as blocked, passed, or included in the white list for that rule.
 - If you select a library category from the Blocked Categories, Pass Categories, or Always Allowed list box, and use the right arrow (>) or left arrow (<) to move that category to another list box, the **Available Filter Levels** pull-down menu changes to “Custom Profile”.

 **TIP:** Multiple categories can be selected by clicking each category while pressing the Ctrl key on your keyboard. Blocks of categories can be selected by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category.

2. Click the “Pass” or “Block” radio button to specify whether all **Uncategorized Sites** should pass or be blocked.
3. Click **Apply** to apply your settings at the entity’s filtering level.

Redirect URL

Click the Redirect URL tab to display the Redirect URL page of the Profile window:

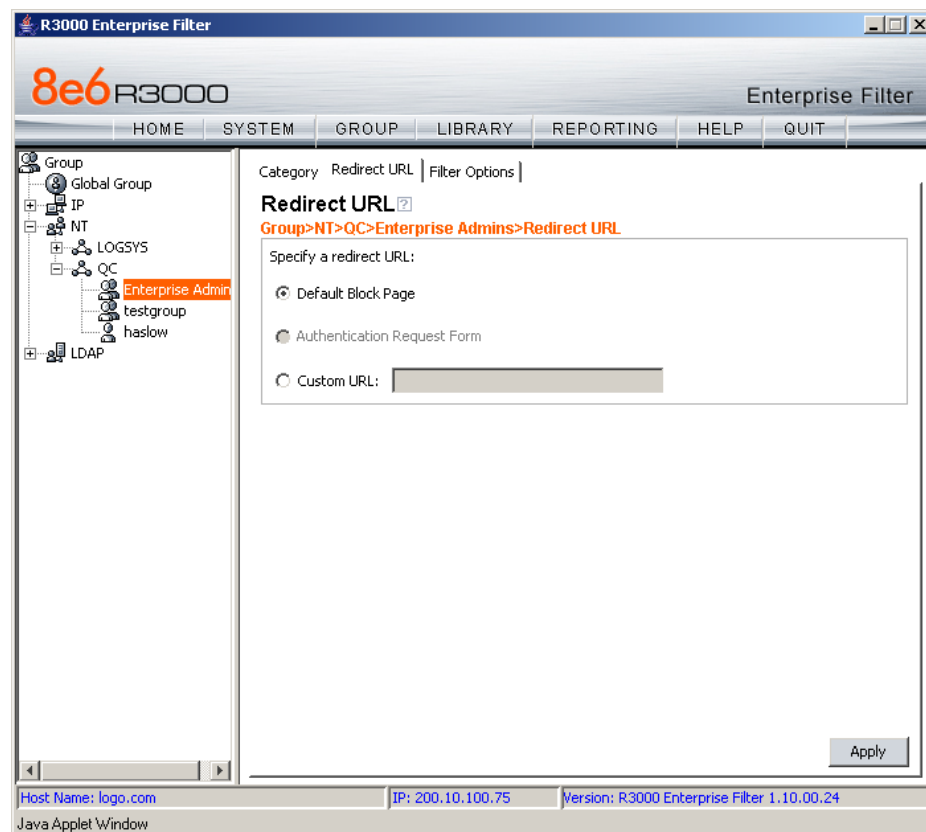


Fig. 3-13 Group Profile window, Redirect URL tab

Redirect URL is used for specifying the URL to be used for redirecting users who attempt to access a site or service set up to be blocked.

1. Specify the type of redirect URL to be used: “Default Block Page”, or “Custom URL”.

If “Custom URL” is selected, enter the redirect URL in the corresponding text box. Users will be redirected to the designated page at this URL instead of the block page.

2. Click **Apply** to apply your settings.

Filter Options

Click the Filter Options tab to display the Filter Options page of the Profile window:

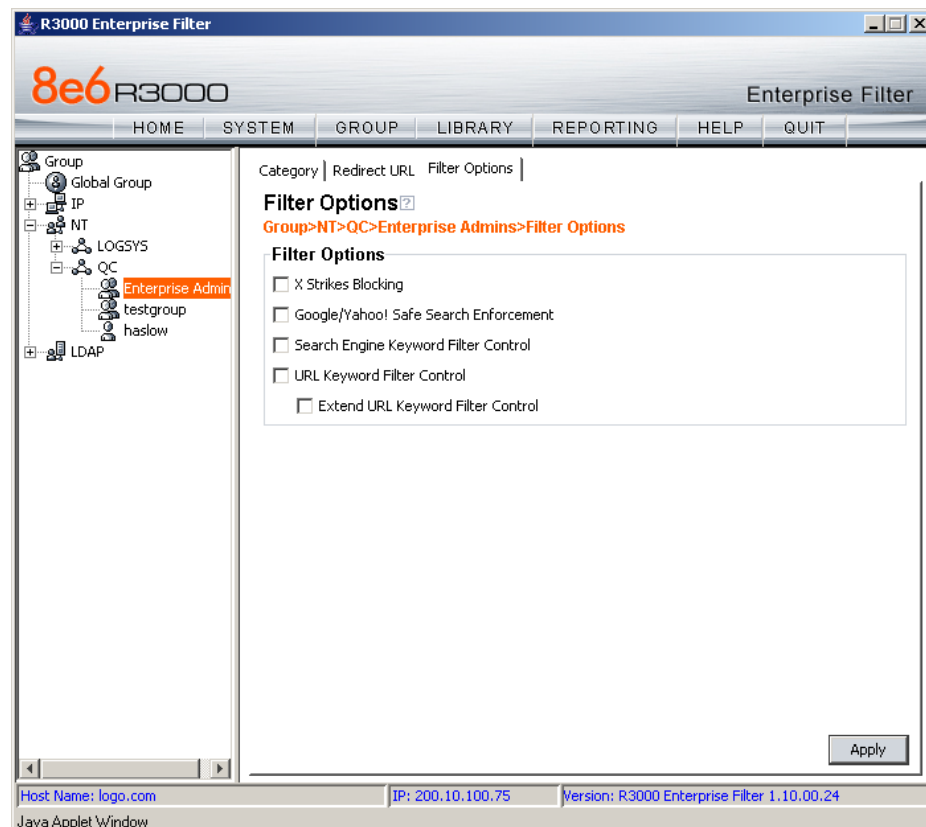


Fig. 3-14 Group Profile window, Filter Options tab

Filter Options is used for specifying which filter option(s) will be applied to the entity's filtering profile.

1. Click the checkbox(es) corresponding to the option(s) to be applied to the filtering profile: "X Strikes Blocking", "Google/Yahoo! Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control". If URL Keyword Filter Control is selected, the "Extend URL Keyword Filter Control" option can be selected.



NOTE: See the *R3000 User Guide* for information about Filter Options.

2. Click **Apply** to apply your settings.

Remove an entity's profile from the tree

To remove a group or member's profile from the tree, select the profile in order to open the pop-up menu, and choose Remove.

CHAPTER 4: LDAP AUTHENTICATION SETUP

Create an LDAP Domain

In the Group section of the console, add an LDAP domain that contains entities to be authenticated.

Add the LDAP domain

1. Click LDAP in the control panel to open the pop-up menu, and select Add Domain to open the Create LDAP Domain dialog box:

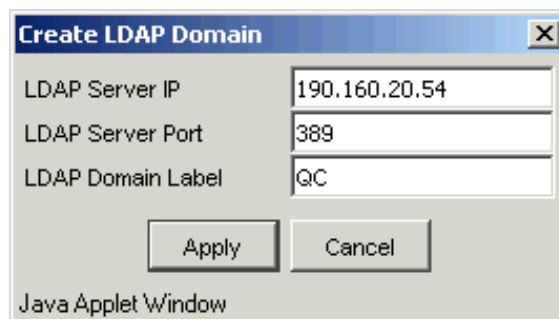
A screenshot of a Java Applet Window titled "Create LDAP Domain". It contains three text input fields: "LDAP Server IP" with the value "190.160.20.54", "LDAP Server Port" with the value "389", and "LDAP Domain Label" with the value "QC". Below the fields are two buttons: "Apply" and "Cancel". The window has a standard title bar with a close button (X) in the top right corner.

Fig. 4-1 Create LDAP Domain box

2. In the **LDAP Server IP** field, enter the IP address of the authentication server.
3. In the **LDAP Server Port** field, enter the LDAP server port number. By default, enter **389**.
4. In the **LDAP Domain Label** field, enter the name of the LDAP domain. This entry does not need to match the NetBIOS name.
5. Click **Apply** to add the domain to the tree. This action takes you directly to the LDAP domain window (see View, modify, enter LDAP domain details).

Refresh the LDAP branch

Click LDAP in the control panel to open the pop-up menu, and select **Refresh** whenever changes have been made in this branch of the tree.

View, modify, enter LDAP domain details

Double-click LDAP in the control panel to open the LDAP branch of the Group tree. Select the LDAP domain you added, and choose Domain Details from the pop-up menu to display the default Type tab of the LDAP Domain Details window:

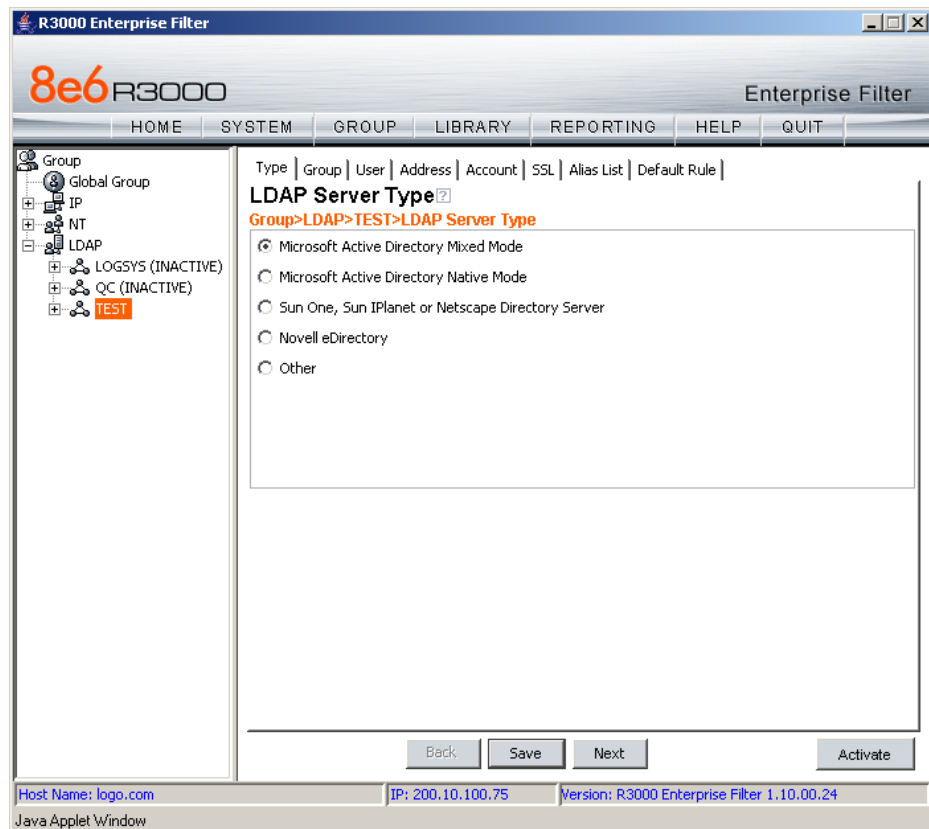


Fig. 4-2 Domain Details window, Type tab

The LDAP domain window is comprised of the following wizard tabs: Type, Group, User, Address, Account, SSL, Alias List, and Default Rule. By going through the entire wizard, domain details are established for the LDAP domain, preparing the LDAP domain for group and user filtering profile setup. After all entries are made on the wizard tabs, the domain can be activated.



WARNING: *The instructions in this user guide have been documented based on standard default settings in LDAP for Microsoft Active Directory Services. The suggested entries and examples may not be applicable to all other server types, or if any changes have made to default settings on the LDAP Active Directory server.*

LDAP Server Type

Based on the entries made when creating the LDAP domain, the R3000 will attempt to auto-detect the type of server being used, and if successfully detected, the appropriate LDAP Server Type radio button will be selected on the Type tab.

- The following options are available: “Microsoft Active Directory Mixed Mode”, “Microsoft Active Directory Native Mode”, “Sun One, Sun IPlanet or Netscape Directory Server”, “Novell eDirectory”, and “Other”. If the server type is not detected, “Other” will be selected.

The server type setting on this tab defines the content that displays on all other tabs of the wizard.



NOTES: *If the server type is changed on this tab, object type settings will be overwritten with the new object type settings. User settings will not be modified.*

If “Novell eDirectory” is selected, and the Novell eDirectory Agent option is enabled in the Enable/Disable Authentication window, the Default Rule tab lets you configure a backup server. See Default Rule for Novell eDirectory.

- Click **Next** to go to the Group tab.



WARNING: The contents of the tabs for User and Group do not normally need to be changed. The settings on these tabs are made automatically when you select the server type at the beginning of the setup process. Unless you have made changes to the Schema of your LDAP server and are sure of the consequences of altering these settings, **do not** alter anything in these tabs. The only action you need to execute on these tabs is to confirm the settings by clicking the **Next** button at the bottom of the window, until you reach the Address tab.

Group Objects

The Group tab is used for including or excluding group objects in the LDAP domain.

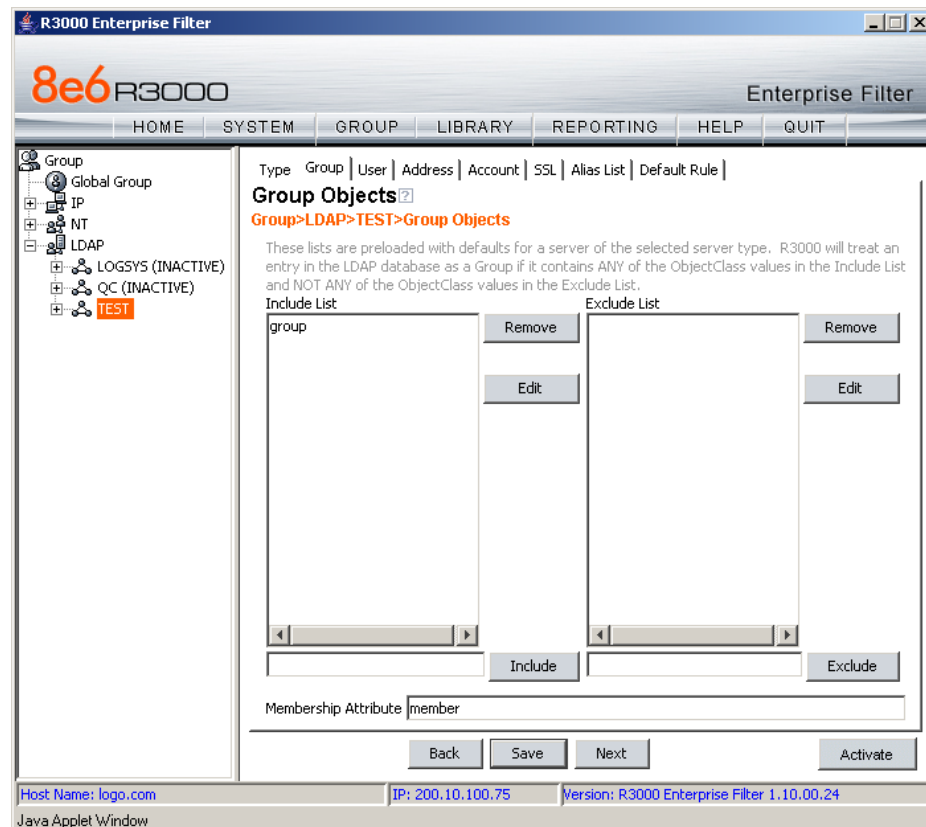


Fig. 4-3 Domain Details window, Group tab

By default, the **Include List** will be populated with appropriate group objects, based on the server type.

- Generally, no action needs to be performed on this tab. However, under special circumstances, a group object can be added or excluded by making an entry in the appropriate field, and then clicking the **Include** or **Exclude** button.
- A group object name can be edited by selecting the group object from the appropriate list box, editing the name in the field, and then clicking the **Edit** button.
- A group object can be removed by selecting the group object and then clicking **Remove**.
- The **Membership Attribute** field is populated by default. The membership attribute is the name of the LDAP attribute in a group record that identifies members of a group.
- If using Active Directory, the “Use Primary Group” checkbox displays on this tab. You may wish to check this box to indicate that profiles based on user groups should be assigned to users.

Click **Next** to go to the User tab.

User Objects

The User tab is used for including or excluding user objects in the LDAP domain.

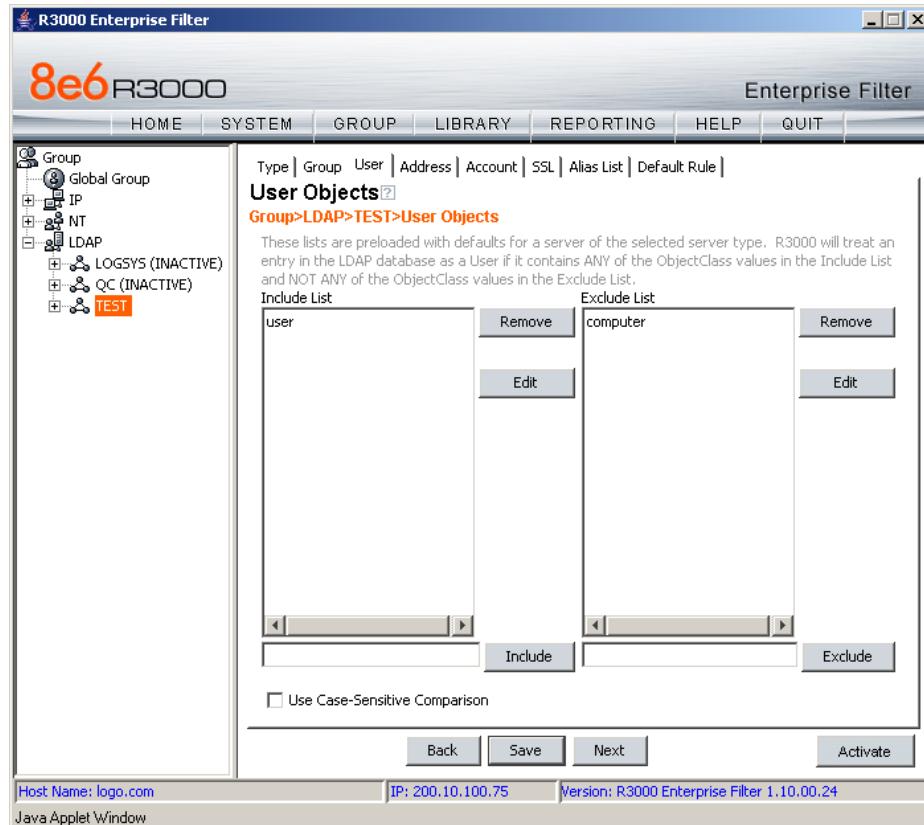


Fig. 4-4 Domain Details window, User tab

By default, the Include List and Exclude List will be populated with appropriate user objects, based on the server type.

- Generally, no action needs to be performed on this tab. However, under special circumstances, a user object can be added or excluded by making an entry in the appropriate field, and then clicking the **Include** or **Exclude** button.

- A user object name can be edited by selecting the user object from the appropriate list box, editing the name in the field, and then clicking the **Edit** button.
- A user object can be removed by selecting the user object and then clicking **Remove**.
- If the user DN cannot be auto-detected during the profile setup process, click “Use Case-Sensitive Comparison” to perform a manual comparison check.

Click **Next** to go to the Address tab.

Address Info

The LDAP domain address information populates the Address tab:

R3000 Enterprise Filter

8e6 R3000 Enterprise Filter

HOME SYSTEM GROUP LIBRARY REPORTING HELP QUIT

Type | Group | User | Address | Account | SSL | Alias List | Default Rule |

Address Info ?

Group>LDAP>TEST>Address Info

Group: Global Group

- IP
- NT
- LDAP
 - LOGSYS (INACTIVE)
 - QC (INACTIVE)
 - TEST**

Server DNS Name: 2000qcserver.qc2domain.local

Server IP Address: 190.160.20.54

DNS Domain Name:

NETBIOS Domain Name:

Server LDAPS Port: 636

Server LDAP Port: 389

LDAP Query Base: DC=qc2domain,DC=local

Back Save Next Activate

Host Name: logo.com IP: 200.10.100.75 Version: R3000 Enterprise Filter 1.10.00.24

Java Applet Window

Fig. 4-5 Domain Details window, Address tab



NOTE: If the DNS settings are not published in the LDAP directory, the **Server DNS Name**, **DNS Domain Name**, and **LDAP Query Base** fields will not be populated automatically. Functioning forward and reverse DNS name resolution is one of the requirements for LDAP authentication. Please ensure the correct DNS settings are set.

- The **Server DNS Name** field should contain the DNS name of the server. If this field is already populated, it may need to be edited if there is more than one DNS server available.



NOTES: If your LDAP server's name is not a resolvable, fully qualified DNS name, you may be able to enter the domain name.

If using a Novell server, be sure the Server DNS Name exactly matches the name on the SSL certificate that will be uploaded to the server.

- The **Server IP Address** that displays by default is the one that was entered in the LDAP Server IP field of the Create LDAP Domain dialog box.
- The **DNS Domain Name** should be the DNS name of the LDAP domain, such as Yahoo.com, and may need to be edited if the entire domain name does not display by default.



NOTES: If your LDAP server's name is not a resolvable, fully qualified DNS name, you may be able to enter the domain name.

If using a Novell server, be sure the DNS Domain Name exactly matches the name on the SSL certificate that will be uploaded to the server.

- If necessary, the **NETBIOS Domain Name** can be entered.
- By default, 636 displays in the **Server LDAPS Port** field.
- By default, the value that was entered in the LDAP Server Port field of the Create LDAP Domain dialog box displays in the **Server LDAP Port** field.

- By default, the **LDAP Query Base** displays the root of the LDAP database to query using the LDAP Syntax, i.e. DC=domain,DC=com. The entry in this field is case sensitive and should be edited, if necessary.

If this field is not populated, enter the LDAP query base.

Click **Next** to go to the Account tab.

Account Info

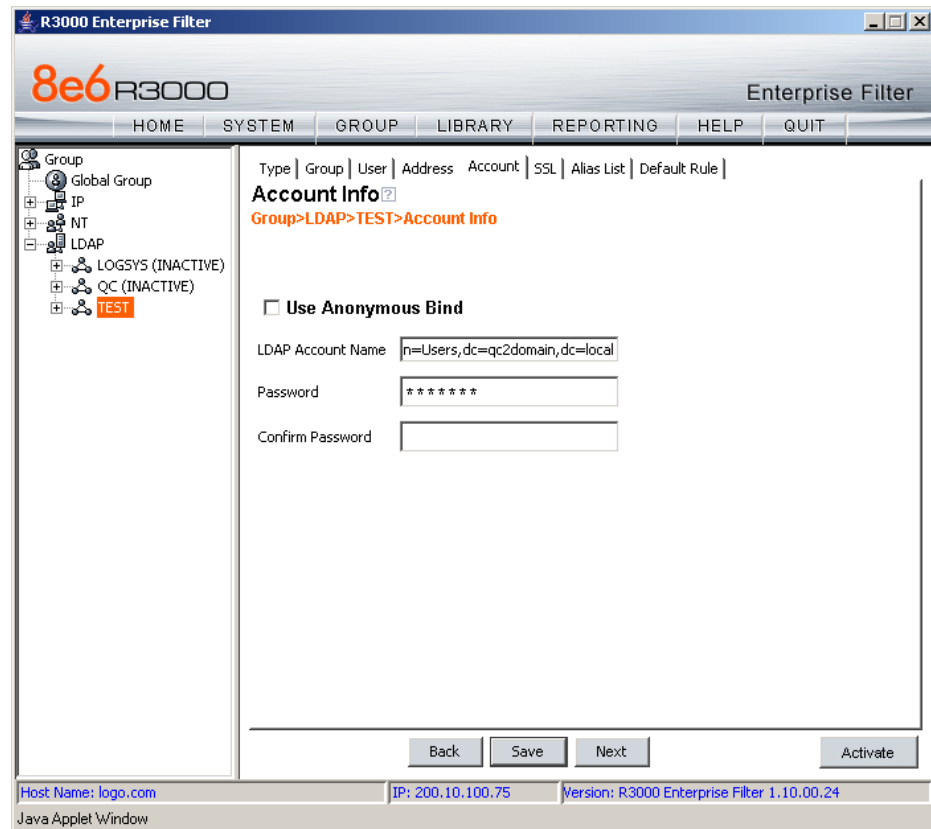


Fig. 4-6 Domain Details window, Account tab

1. If your LDAP database does not require a username to be provided in order to bind to the LDAP database, click the “Use Anonymous Bind” checkbox to grey out the fields in this tab.

Otherwise:

- Enter the authorized user's full LDAP Distinguished Name in the **LDAP Account Name** field.

For example:

cn=Administrator,cn=Users,dc=qc2domain,dc=local

- Enter the password in the **Password** and **Confirm Password** fields.

2. Click **Next** to go to the SSL tab.

SSL Settings

SSL settings should be made if your network requires a secure connection from the R3000 to the LDAP server.

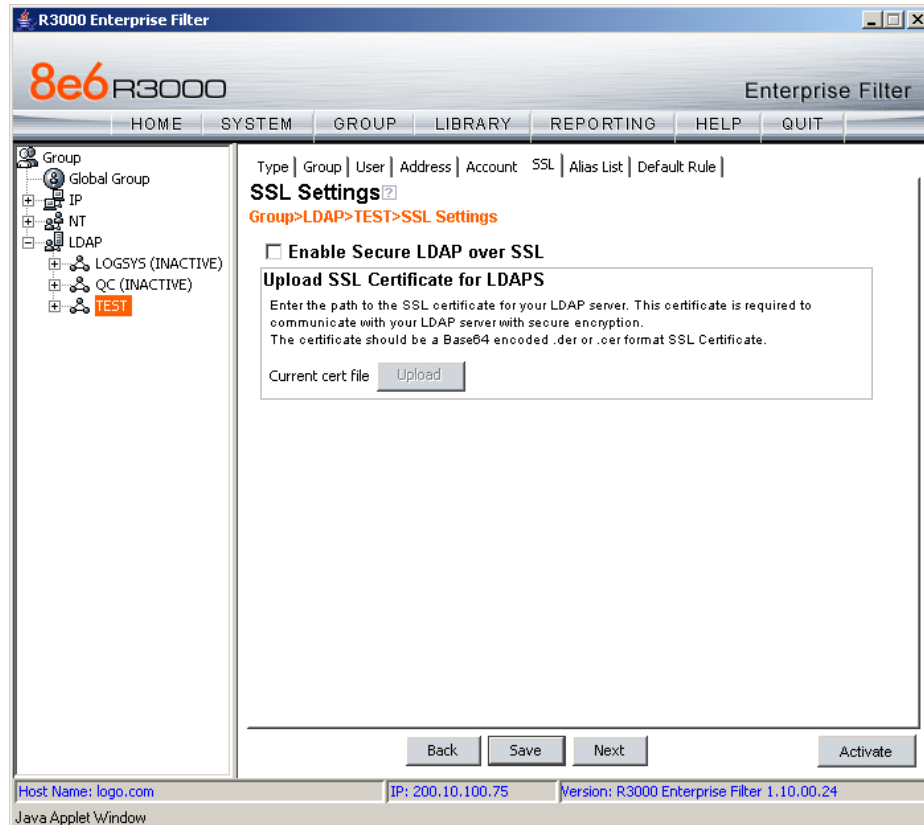


Fig. 4-7 Domain Details window, SSL tab

 **NOTE:** See Appendix E: Obtain or Export an SSL Certificate for information on how to obtain a Sun ONE server's SSL certificate, or how to export an Active Directory or Novell server's SSL certificate to your desktop and then upload it to the R3000.

1. If applicable, click in the "Enable Secure LDAP over SSL" checkbox. This action activates the Upload button.
2. Click the **Upload** button to open the Upload SSL Certificate for LDAPS pop-up window:

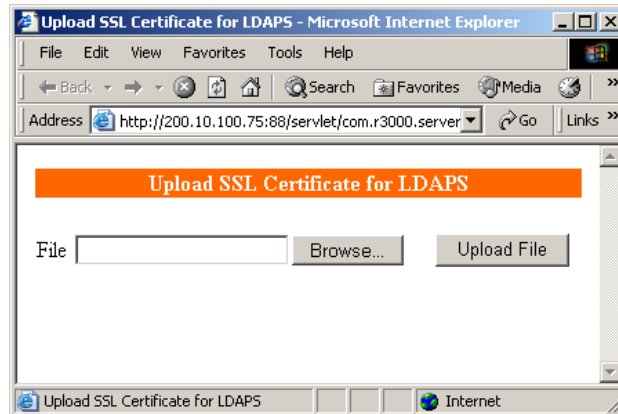


Fig. 4-8 Upload SSL Certificate for LDAPS

3. Click **Browse** to open the Choose file window and select the R3000 server's SSL certificate.
4. Click **Upload File** to upload the SSL certificate to the R3000 server.



WARNING: If using a Novell server, be sure the name on the SSL certificate (to be uploaded to the server) matches the Server DNS Name entered in the Address Info tab.

5. Click **Next** to go to the Alias List tab.

Alias List

The Alias List will be automatically populated if the Account Name was entered in the Account tab. This list includes all alias names for the domain that will be included in the Alias pull-down menu in the Authentication Request Form.

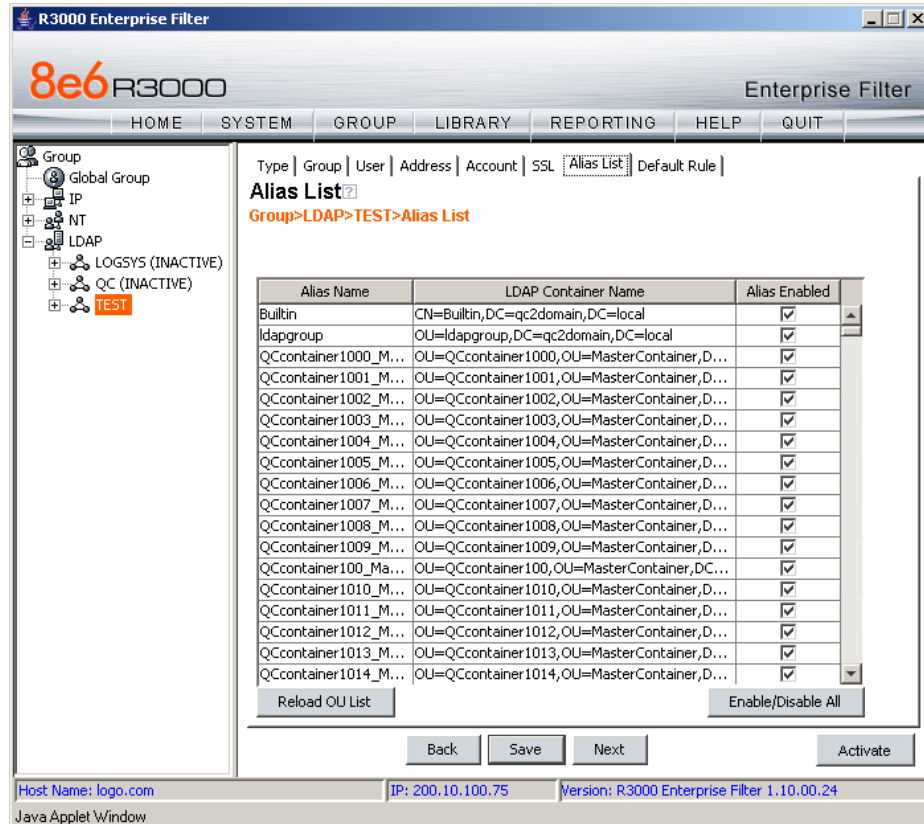


Fig. 4-9 Domain Details window, Alias List tab

However, if there are many alias names to be loaded, the tab initially displays without any data and the Search in Progress box opens:

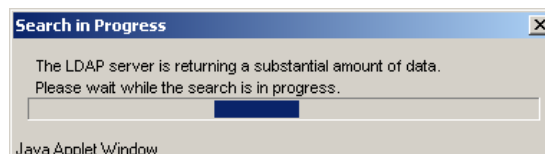


Fig. 4-10 Search in Progress box

After the search is completed, the Search in Progress box closes, and the list displays the Alias Name and the corresponding LDAP Container Name.



NOTE: *If the alias list does not display, double-check the settings on the other tabs and verify that all of your settings are correct.*

The following actions can be performed on this tab:

- An Alias Name can be edited by double-clicking the Alias Name in the designated row, and then making your modifications.
- If an Organizational Unit (OU) has been deleted from the LDAP directory but has already been added to the alias list, the list can be reloaded by clicking the **Reload OU List** button. When clicking this button, the Search in Progress box opens and the domain becomes inactive and will need to be reactivated.
- By default, all items are selected for inclusion in the alias list, as indicated by a check mark in the Alias Enabled checkbox. To deselect an item, click the checkbox to remove the check mark.
- To select or deselect all items in the list, click the **Enable/Disable All** button. This button lets you toggle between these two operations.

Click **Next** to go to the Default Rule tab.

Default Rule

The Default Rule applies to any authenticated user in the LDAP domain who does not have a filtering profile.

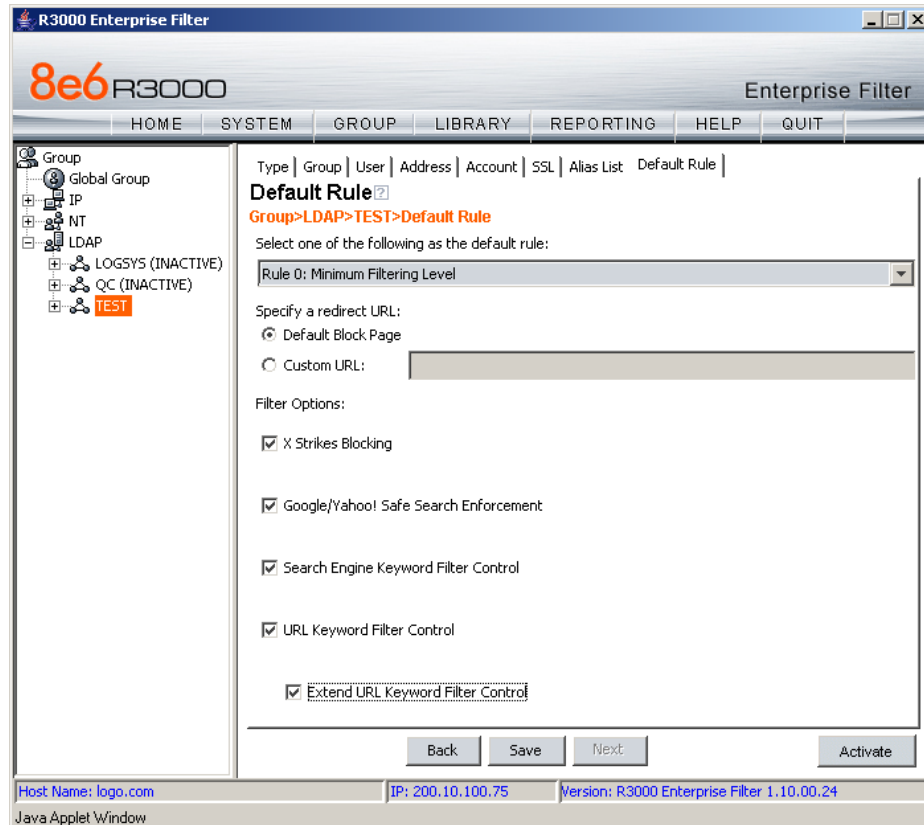


Fig. 4-11 Domain Details window, Default Rule tab



NOTE: If using Novell eDirectory, see *Default Rule for Novell eDirectory*.

The tab is comprised of the following components that can be modified:

- By default, “Rule0” is the default rule. This rule can be changed by making another selection from the pull-down menu.
- To specify the type of redirect URL to be used for users who do not have a filtering profile, click the radio button corresponding to “Default Block Page”, or “Custom URL”.

If Custom URL is selected, enter the redirect URL in the text box.

- Click the checkbox(es) corresponding to the option(s) to be applied to the filtering profile: “X Strikes Blocking”, “Google/Yahoo! Safe Search Enforcement”, “Search Engine Keyword Filter Control”, “URL Keyword Filter Control”. If URL Keyword Filter Control is selected, the “Extend URL Keyword Filter Control” option can be selected.

After all entries have been made in the tabs, click **Activate** to activate the domain.



NOTE: To enter profile information for LDAP groups and users, see *Create, Maintain LDAP Profiles*.

Default Rule for Novell eDirectory

If “Novell eDirectory” was selected for the LDAP Server Type, and the Novell eDirectory Agent option was enabled in the Enable/Disable Authentication window in the System section of the console, the Default Rule tab includes buttons for configuring a backup server to be used in the event the primary server cannot be accessed.

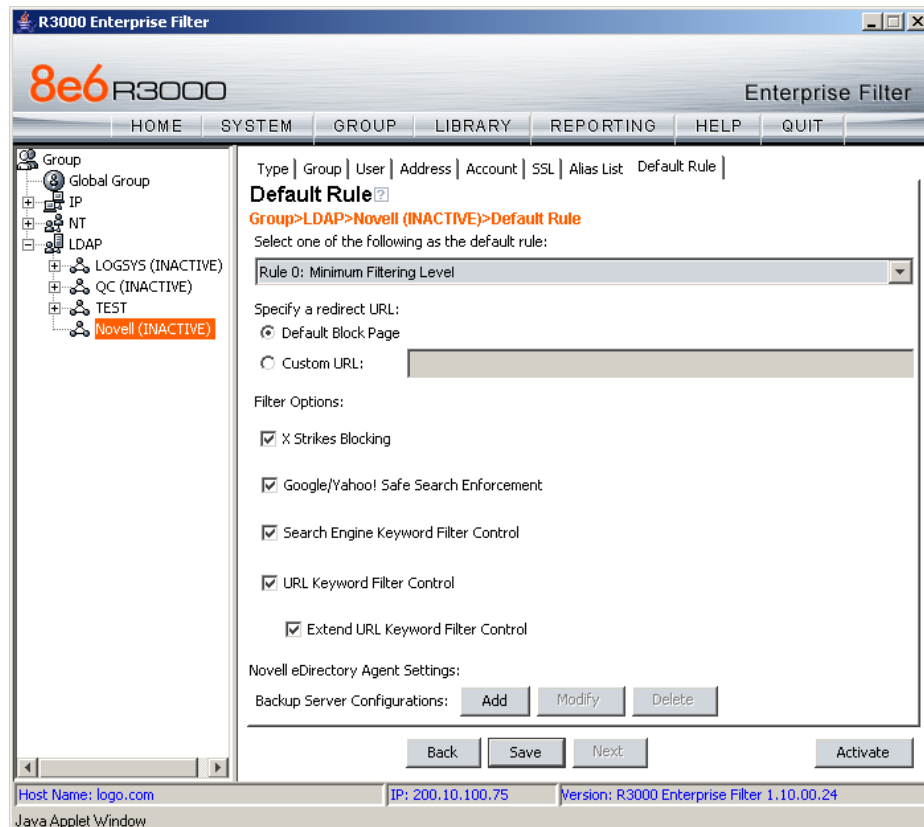


Fig. 4-12 Domain Details window, Default Rule with Novell eDirectory

Configure a backup server

To add a backup server's settings:

1. Click **Add** to open the Backup Server Configuration wizard pop-up window:

Backup Server Configuration

Address | Account | SSL |

Address Info

Group>LDAP>Novell (INACTIVE)>Address Info

Server DNS Name

Server IP Address

DNS Domain Name

NETBIOS Domain Name

Server LDAPS Port

Server LDAP Port

LDAP Query Base

Back Save Next Close

Java Applet Window

Fig. 4-13 Backup Server Configuration, Address Info



NOTE: The **Back** and **Save** buttons can be clicked at any time during the wizard setup process. Click **Close** to close the wizard pop-up window.

2. Enter, edit, or verify the following criteria:

- **Server DNS Name** - DNS name of the LDAP server, such as server.logo.local



NOTES: If your LDAP server's name is not a resolvable, fully qualified DNS name, you may be able to enter the domain name.

Be sure the Server DNS Name exactly matches the name on the SSL certificate that will be uploaded to the server.

- **Server IP Address** - IP address of the server, such as 100.10.150.30
- **DNS Domain Name** - DNS name of the LDAP domain, such as logo.local



NOTES: If your LDAP server's name is not a resolvable, fully qualified DNS name, you may be able to enter the domain name.

Be sure the DNS Domain Name exactly matches the name on the SSL certificate that will be uploaded to the server.

- **NETBIOS Domain Name** - an entry in this field is optional
- **Server LDAPS Port** - by default, 636 displays in this field
- **Server LDAP Port** - by default, the value that was entered in the LDAP Server Port field of the Create LDAP Domain dialog box displays in the field
- **LDAP Query Base** - root of the LDAP database to query using the LDAP Syntax, i.e. DC=domain,DC=com.



TIP: The entry in this field is case sensitive.

3. Click **Next** to go to the Account tab:

Fig. 4-14 Backup Server Configuration, Account Info

4. Enter, edit, or verify the following criteria:

- “Use Anonymous Bind” - click this checkbox to grey out the fields in this tab, if your LDAP database does not require a username to be provided in order to bind to the LDAP database
- Otherwise:

- a. Enter the authorized user's full LDAP Distinguished Name in the **LDAP Account Name** field.

For example:

cn=Administrator,cn=Users,dc=qc2domain,
dc=local

- b. Enter the password in the **Password** and **Confirm Password** fields.

5. Click **Next** to go to the SSL tab:

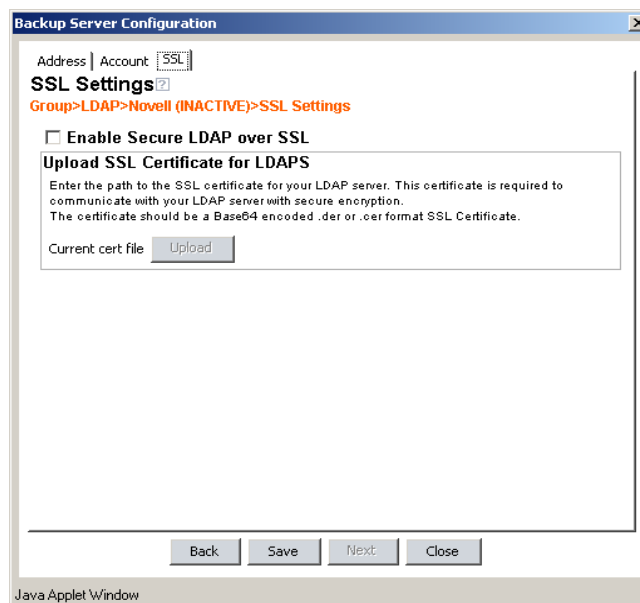


Fig. 4-15 Backup Server Configuration, SSL Settings

SSL settings should be made if your network requires a secure connection from the R3000 to the LDAP server.



NOTE: See Appendix E: Obtain or Export an SSL Certificate for information on how to export a Novell server's SSL certificate to your desktop and then upload it to the R3000.

- a. If applicable, click in the "Enable Secure LDAP over SSL" checkbox. This action activates the Upload button.
- b. Click the **Upload** button to open the Upload SSL Certificate for LDAPS pop-up window (see Fig. 4-8).

- c. Click **Browse** to open the Choose file window and select the R3000 server's SSL certificate.
- d. Click **Upload File** to upload the SSL certificate to the R3000 server.



WARNING: Be sure the name on the SSL certificate (to be uploaded to the server) matches the Server DNS Name entered in the Address Info tab.

6. After all entries are made using the wizard, click **Save**.
7. Click **Close** to close the wizard pop-up window.

Modify a backup server's configuration

1. On the Default Rult tab for a Novell eDirectory server set up in the LDAP tree menu, click **Modify** to open the Backup Server Configuration wizard pop-up window.
2. Click the tab(s) in which to make edits for the backup server: Address, Account, SSL.
3. Make the necessary edits.
4. Click **Save**.
5. Click **Close** to close the wizard pop-up window.

Delete a backup server's configuration

On the Default Rult tab for a Novell eDirectory server set up in the LDAP tree menu, click **Delete** to remove the backup server's configuration.

Delete a domain

To delete a domain profile, choose Delete from the LDAP domain menu. This action removes the domain from the tree.

Set up LDAP Domain Groups, Members

In the control panel, the LDAP domain branch of the tree menu includes options for setting up groups and/or members in the domain so that filtering profiles can later be created. The following options are used in this setup process: Select Group/Member from Domain, Set Group Priority, Manually Add Member, Manually Add Group, and Upload User/Group Profile.

Add LDAP groups, users to the tree

Before you can create filtering profiles for groups and/or members in a domain, you must first add the groups and/or members to the tree list for that domain.

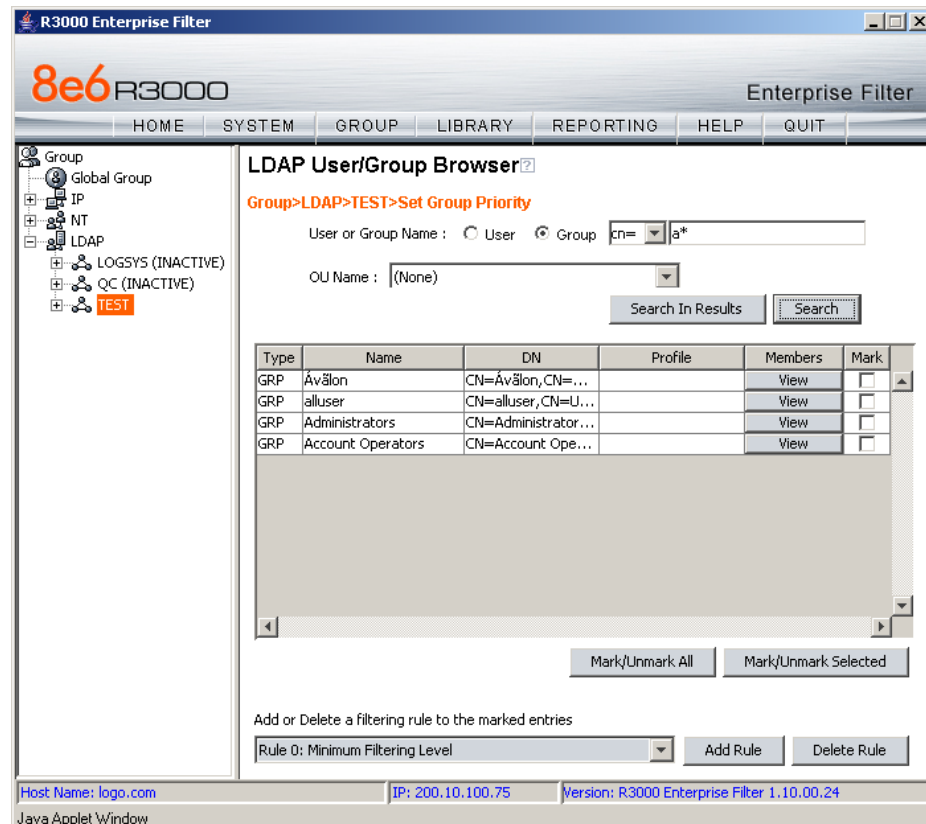


Fig. 4-16 LDAP User/Group Browser window

Select the LDAP domain, and choose **Select Group/Member from Domain** from the pop-up menu to display the LDAP User/Group Browser window (see Figure 4-12).

This window is used for retrieving the names of groups or users from an LDAP domain so that a filtering profile can be assigned.



NOTE: See *Appendix C: LDAP Server Customizations if using an OpenLDAP server*.

Perform a basic search

1. Specify the type of search by clicking the “User” or “Group” radio button.
2. Choose either “cn=” (common name) or “uid=” (user ID) from the pull-down menu for the attribute type used in the LDAP directory.
3. In the **User or Group Name** field, input the group or username exactly as it was entered on the LDAP server, or enter a partial name followed by the asterisk (*) wild-card.
4. Click **Search** to display rows of results in the grid below. The following information is included for each entity: Type (USR or GRP), Name (as entered on the LDAP server), DN string, Profile (Rule number, if assigned), View button, check box.

Options for search results

After performing a search, you can do either of the following:

- **Narrow your search** – To narrow your search, make a selection from the **OU Name** pull-down menu, and then click **Search In Results**. This will limit your results to the specified section of the LDAP database.

- Search within existing results – To search within the list of records returned by your initial query, change your search criteria, and then click **Search In Results**. This can speed up searches when the LDAP server is slow to respond.

The **View** button in the Members column is used for either querying the list of groups in which a user is a member, or the list of users who are members of a Group Record.

To select or deselect all items in the grid, click **Mark/Unmark All**.

To select or deselect all highlighted items in the grid, click **Mark/Unmark Selected**. This feature works only if items are first selected in the grid by clicking on them.

- Multiple items are selected by clicking one item, and then pressing the **Ctrl** key on your keyboard and clicking another item.
- A block of multiple items is selected by clicking the first item in the block, then pressing the **Shift** key on your keyboard, and then clicking the last item in the block.

Apply a filtering rule to a profile

To apply a filtering rule to an entity in the grid:

1. Go to the Mark column and click the checkbox for that entity.
2. Select a filtering rule from the drop-down menu.
3. Click **Add Rule** to display the selected Rule number in the Profile column.

When the LDAP branch of the tree is refreshed, all entities with rules applied to them appear in the tree.

Delete a rule

To delete a rule from a profile, the entity must currently display in the grid and have a rule assigned to the profile.

1. Click the Mark checkbox for the entity.
2. Click **Delete Rule** to remove the entity's profile from the tree.

Specify a group's filtering profile priority

1. Select the LDAP domain, and choose Set Group Priority from the pop-up menu to display the Set Group Priority window:

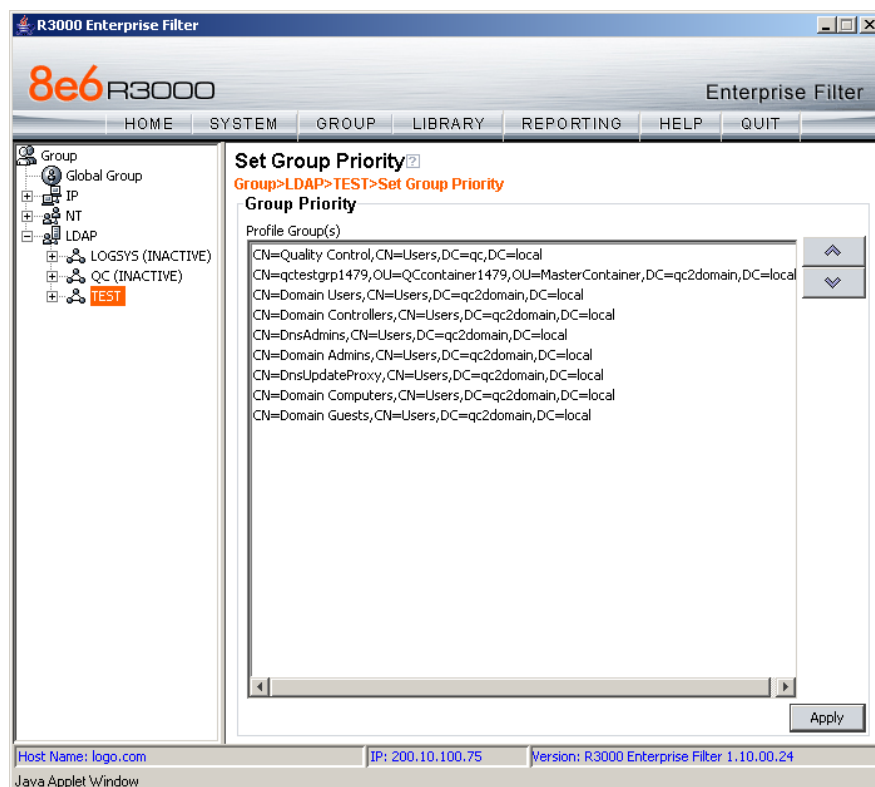


Fig. 4-17 Set Group Priority window

This window is used for designating which group profile will be assigned to a user when he/she logs in. If a user is a member of multiple groups, the one that is positioned highest in the list is applied.



NOTES: Groups automatically populate the Profile Group(s) list box, if these groups have one or more identical users and were added to the tree list via the Select Groups/Members from Domain window.

An entry for the Group Priority list is added to the end of the list when the group profile for that group is added to the R3000, and is removed automatically when you delete the profile.

2. To change the order of groups in the list:
 - a. Select a group from the Profile Group(s) list box.
 - b. Use the up or down arrow button to move that group up or down in the list.
 - c. Click **Apply** to apply your settings.

Manually add a user's name to the tree

1. Select the LDAP domain, and choose Manually Add Member from the pop-up menu to open the Manually Add Member dialog box:

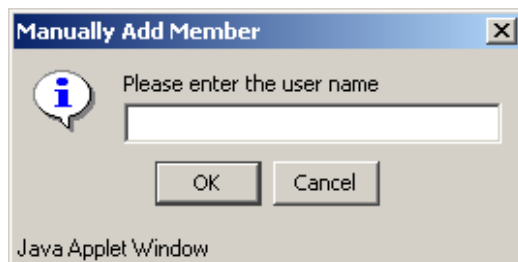


Fig. 4-18 Manually Add Member box

This dialog box is used for adding a username to the tree list, so that a filtering profile can be defined for that user.

2. Enter the username in the text box.

 **TIP:** LDAP usernames should be input exactly as entered as entered for the LDAP Distinguished Name.

Examples:

CN=Jane Doe, CN=Users, DC=qc, DC=local

CN=Public\, Joe Q., OU=Users, OU=Sales, DC=qc, DC=local

CN=Doe\, John, CN=Users, DC=qc, DC=local

3. Click **OK** to add the username to the domain's section of the tree.

 **NOTE:** See *Add or maintain an entity's profile under Create and Maintain LDAP Profiles* for information on defining the filtering profile for the user.

Manually add a group's name to the tree

1. Select the LDAP domain, and choose Manually Add Group from the pop-up menu to open the Manually Add Group dialog box:

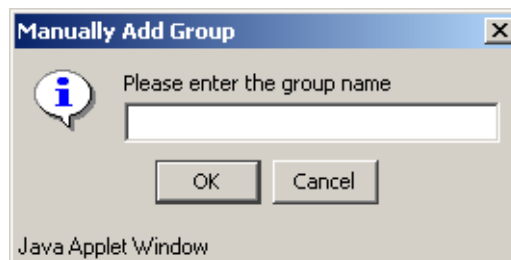


Fig. 4-19 Manually Add Group box

This dialog box is used for adding a group name to the tree list, so that a filtering profile can be defined for that group.

2. Enter the group's name in the text box, using the entire Distinguished Name format.
3. Click **OK** to add the group name to the domain's section of the tree.



NOTE: See *Add or maintain the entity's profile* under *Create and Maintain LDAP Profiles* for information on defining the filtering profile for the group.

Upload a file of filtering profiles to the tree

1. Select the LDAP domain, and choose Upload User/Group Profile from the pop-up menu to open the Upload User/Group Profile window:

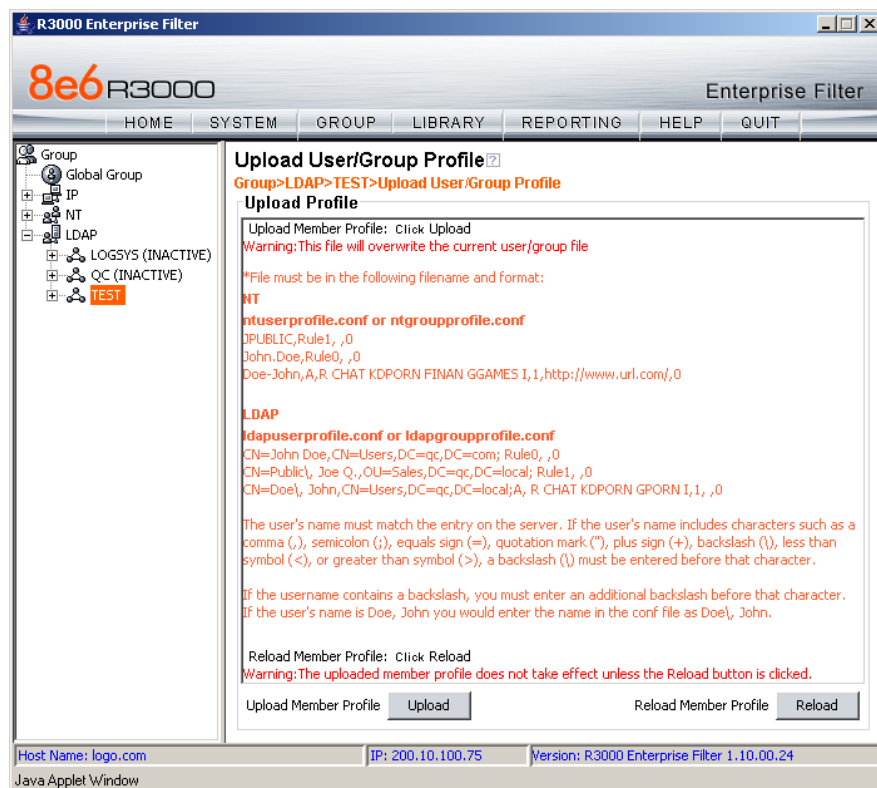


Fig. 4-20 Upload User/Group Profile window

This window is used for uploading a file to the tree with user or group names and their associated filtering profiles.

2. Click **Upload** to open the Upload Member Profile File pop-up window:

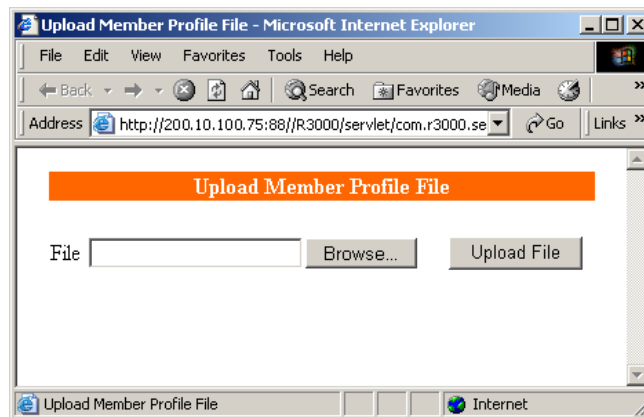


Fig. 4-21 Upload Member Profile File window

3. Click **Browse** to open the Choose file window.
4. Select the file to be uploaded.



WARNING: Any file uploaded to the server will overwrite the existing user/group profile file.

Each user/group profile in the file uploaded to the server **must be** set up in a specified format in order for the profile to be activated on the server. This format differs depending on whether the profiles are user or group profiles. Based on the type of file format used, the file should have the following name:

- **ldapuserprofile.conf** if the file contains LDAP user profiles
- **ldapgroupprofile.conf** if the file contains LDAP group profiles



NOTE: See Appendix A: User/Group File Format and Rules for examples of valid filtering profile formats to use when creating a list of profiles to be uploaded to the server.



WARNING: When uploading a list of profiles to the tree, the user will be blocked from Internet access if the minimum filtering level has not been defined via the Minimum Filtering Level window. If you have just established the minimum filtering level, filter settings will not be effective until the user logs off and back on the server.

5. Click **Upload File** to upload this file to the server. The Upload Successful pop-up window informs you to click Reload in order for these changes to be effective.
6. Click **Reload**.
7. Go to the LDAP branch of the tree, and choose **Refresh** from the LDAP group menu.

Create, Maintain LDAP Profiles

Once an LDAP group or member has been added to the tree, a filtering profile can be created and maintained for that entity. For groups, the following options are available for filtering profile creation and maintenance: Group Member Details, Profile, and Remove. For members, the following options are available for filtering profile creation and maintenance: Profile, and Remove.

Add an LDAP group, member to the tree

Select the LDAP domain, and choose Group Member Details from the pop-up menu to display the Group/Member Details window:

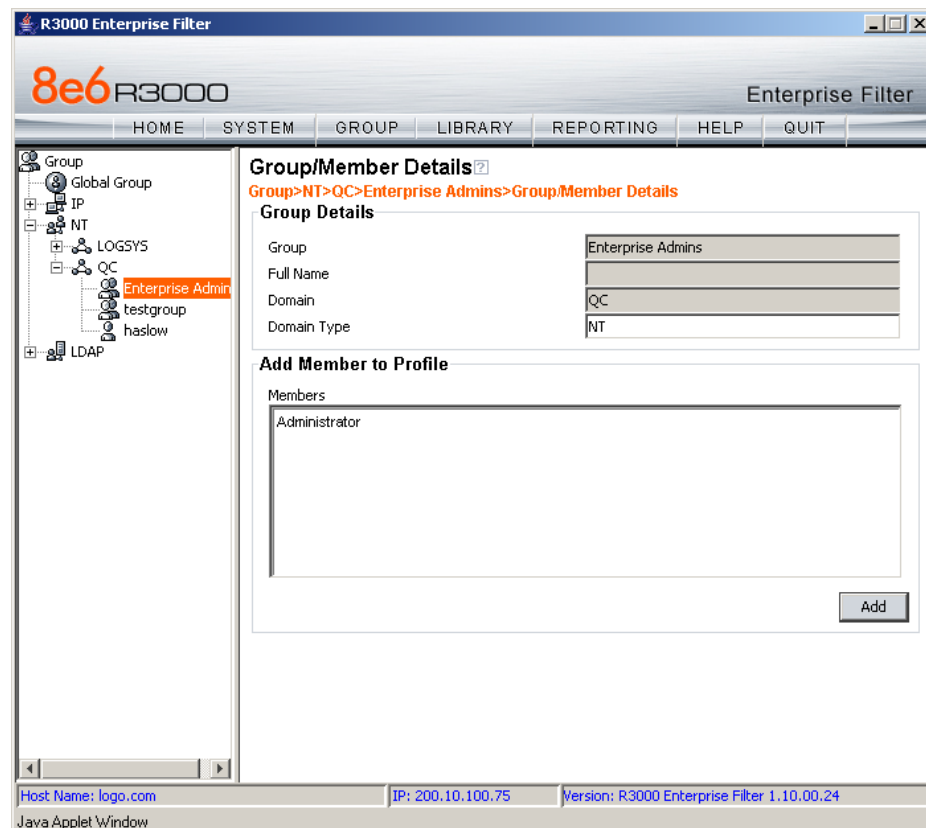


Fig. 4-22 Group Member Details window

This window is used for viewing profile information about a group, and for adding members to a group.

In the Group Details frame, the following details display: **Group** name, **Full Name** (Distinguished Name) of the group, **Domain** name, and **Domain Type**. Members that belong to the group display in the Members list box in the Add Member to Profile frame.

To add a member to the tree list so that a profile can be created for that member:

1. Select the entity from the Members list box.
2. Click **Add**.

Add or maintain an entity's profile

Select the LDAP domain, and choose Profile from the pop-up menu to display the default Category tab of the Profile window:

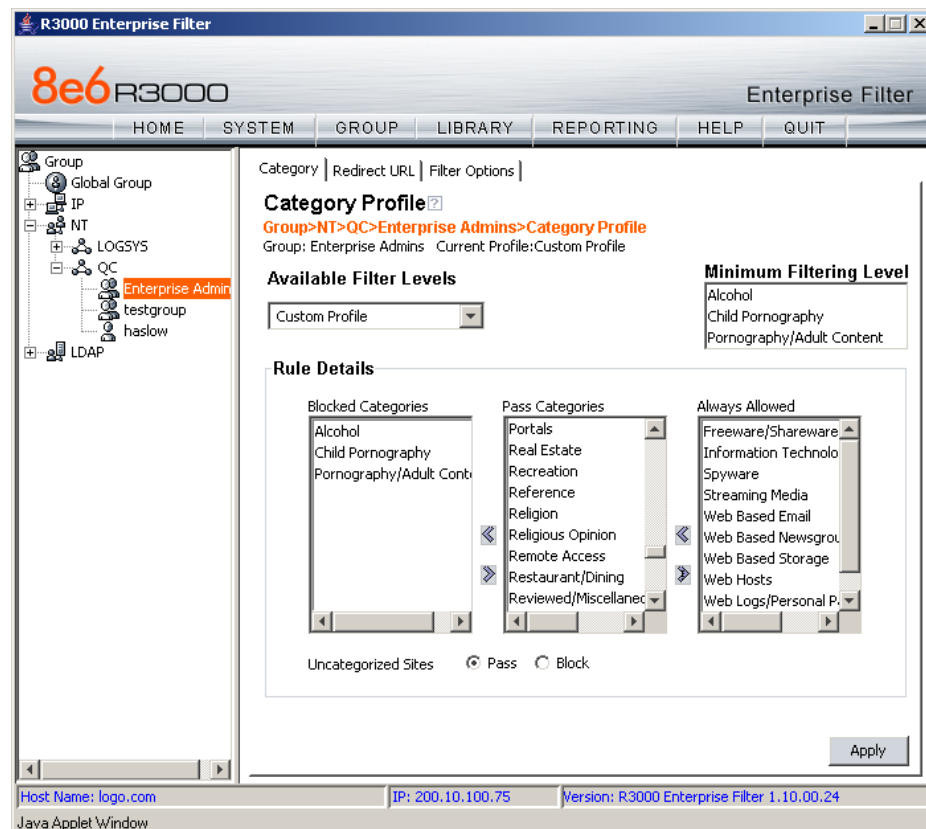


Fig. 4-23 Group Profile window, Category tab

The Profile option is used for viewing/creating the filtering profile of the defined entity (group or member). Entries made in the Category, Redirect URL, and Filter Options tabs comprise the profile string for the entity.

Category Profile

Category Profile is used for creating the categories portion of the filtering profile for the entity.



NOTE: In order to use this tab, filtering rules should already have been set up via the Rules window, accessible from the Global Group options, and the minimum filtering level should already be established. The minimum filtering level is set up in the Minimum Filtering Level window, accessible from the Global Group options.

By default, “Rule0 Minimum Filtering Level” displays in the **Available Filter Levels** pull-down menu, and the Minimum Filtering Level box displays “Child Pornography” and “Pornography/Adult Content”. By default, **Uncategorized Sites** are allowed to Pass.



NOTE: By default, the **Available Filter Levels** pull-down menu also includes these three rule choices: Rule1 BYPASS”, “Rule2 BLOCK Porn”, “Rule3 Block IM and Porn”, and “Rule4 8e6 CIPA Compliance”.

To create the category portion of the entity’s filtering profile:

1. Select a filtering rule from the available choices, and/or select categories to block.
 - If you select a filtering rule from the **Available Filter Levels** pull-down menu, this action automatically populates the Blocked Categories, Pass Categories, and/or Always Allowed list box(es) in the Rule Details frame with library categories set up as blocked, passed, or included in the white list for that rule.
 - If you select a library category from the Blocked Categories, Pass Categories, or Always Allowed list box, and use the right arrow (>) or left arrow (<) to move that category to another list box, the **Available Filter Levels** pull-down menu changes to “Custom Profile”.



TIP: Multiple categories can be selected by clicking each category while pressing the Ctrl key on your keyboard. Blocks of categories can be selected by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category.

2. Click the “Pass” or “Block” radio button to specify whether all Uncategorized Sites should pass or be blocked.
3. Click **Apply** to apply your settings at the entity’s filtering level.

Redirect URL

Click the Redirect URL tab to display the Redirect URL page of the Profile window:

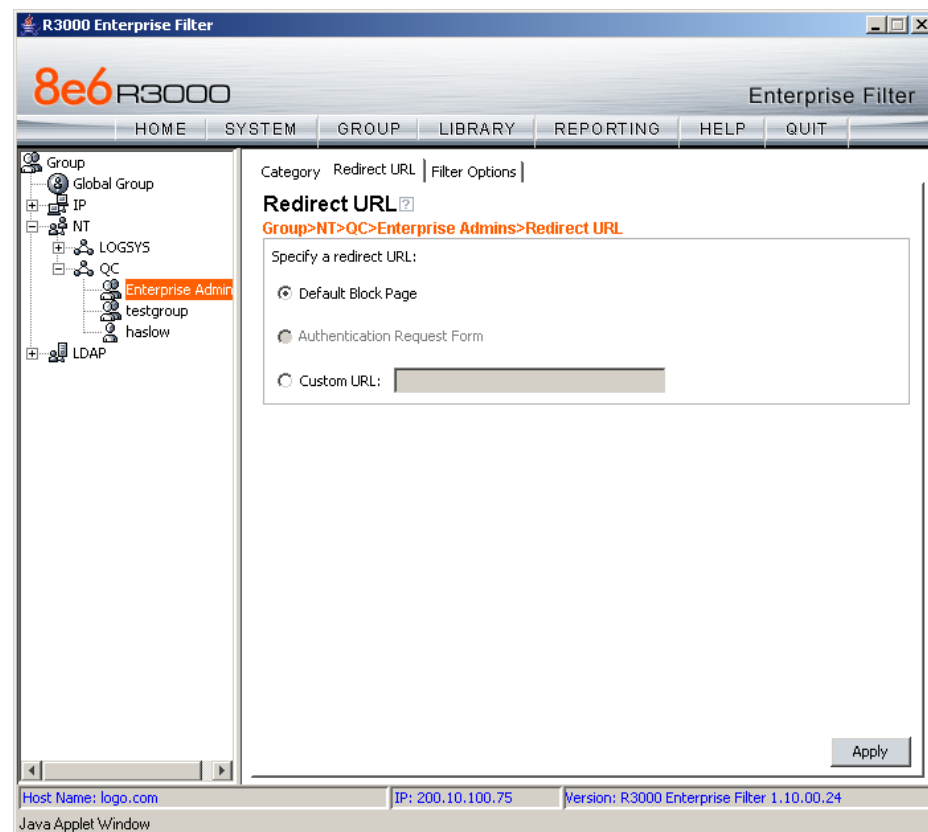


Fig. 4-24 Group Profile window, Redirect URL tab

Redirect URL is used for specifying the URL to be used for redirecting users who attempt to access a site or service set up to be blocked.

1. Specify the type of redirect URL to be used: “Default Block Page”, or “Custom URL”.

If “Custom URL” is selected, enter the redirect URL in the corresponding text box. Users will be redirected to the designated page at this URL instead of the block page.

2. Click **Apply** to apply your settings.

Filter Options

Click the Filter Options tab to display the Filter Options page of the Profile window:

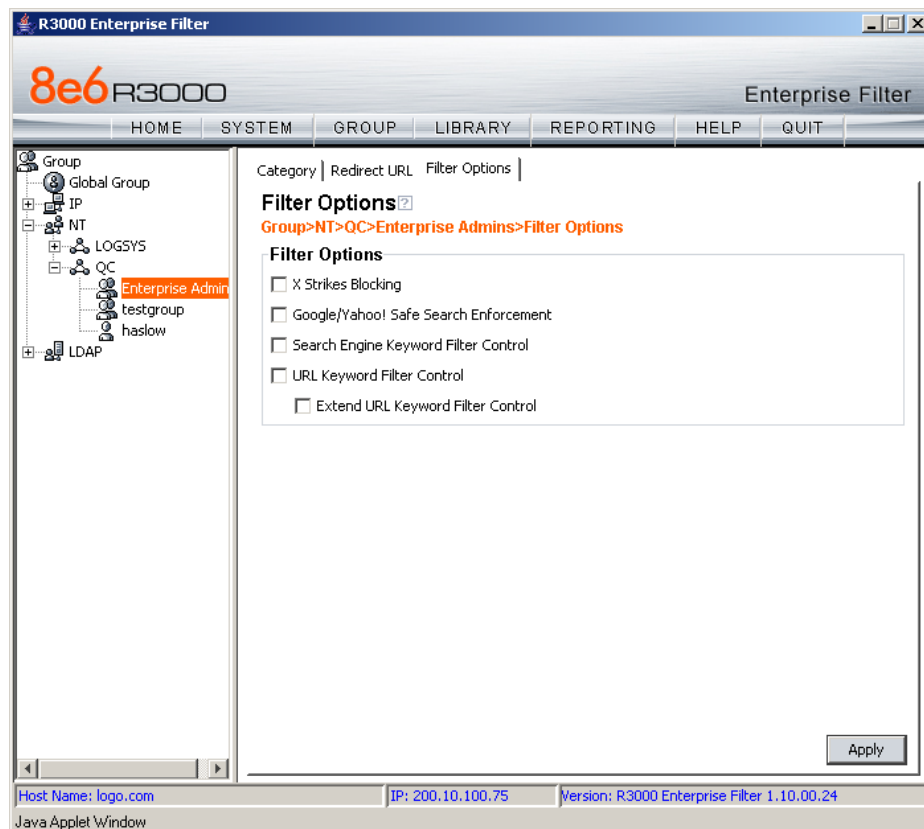


Fig. 4-25 Group Profile window, Filter Options tab

Filter Options is used for specifying which filter option(s) will be applied to the entity's filtering profile.

1. Click the checkbox(es) corresponding to the option(s) to be applied to the filtering profile: "X Strikes Blocking", "Google/Yahoo! Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control", and "Extend URL Keyword Filter Control".



NOTE: See the *R3000 User Guide* for information about Filter Options.

2. Click **Apply** to apply your settings.

Remove an entity's profile from the tree

To remove a group or member's profile from the tree, select the profile in order to open the pop-up menu, and choose Remove.

CHAPTER 5: AUTHENTICATION DEPLOYMENT

This final step of the authentication setup process includes testing authentication settings and activating authentication on the network.

Test Authentication Settings

Before deploying authentication on the network, you should test your settings to be sure the Authentication Request Form login page can be accessed. If properly set up, the Authentication Request Form opens on a user's workstation if the user has been blocked from accessing specified Internet content. This form allows the user to authenticate him/herself in order to access Web content permitted by his/her filtering profile.

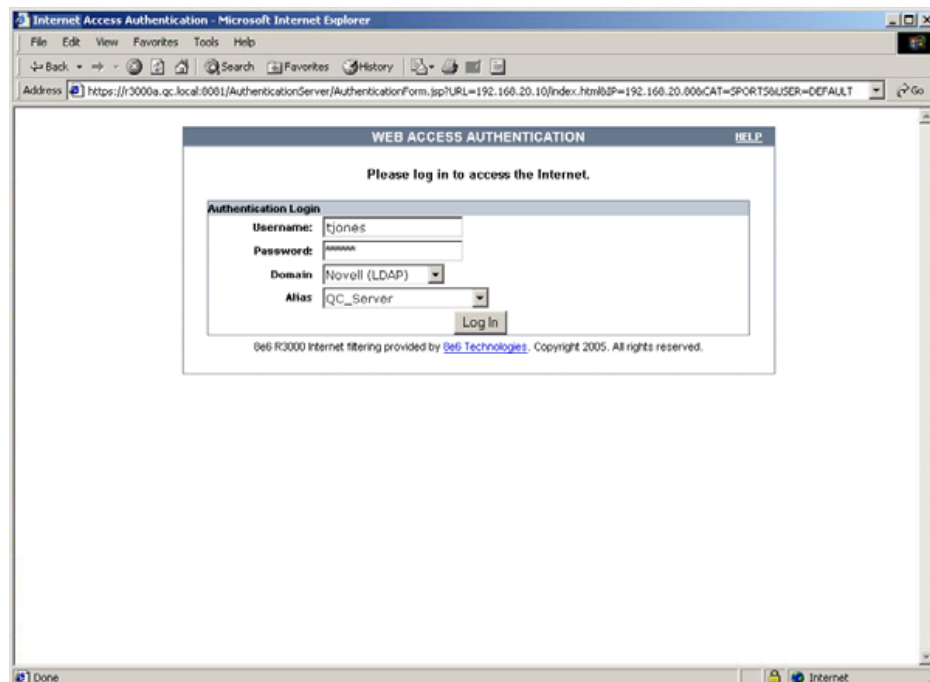


Fig. 5-1 Authentication Request Form



NOTE: *In order to complete the test process, you should be sure you have your own filtering profile set up.*

To verify that authentication is working, do either of the following, based on the Tier you selected:

- **If Tier 2 or Tier 3 Web-based authentication will be used:** Go to the Test Web-based authentication settings sub-section for instructions on testing the Authentication Request Form login page from a single workstation. For this test, you will create an IP profile for the test machine's IP address, and set the Redirect URL for the profile to access the Authentication Request Form.



NOTE: *Before testing Web-based authentication settings, be sure the SSL certificate you created via the System > Authentication > Authentication SSL Certificate window (in Chapter 2) is placed on all workstations of users who will be authenticated. This ensures that users will not receive the Security Alert warning message from the server.*

- **If Tier 1 net use based authentication will be used:** Go to the Test net use authentication settings sub-section for instructions on testing the net use based login command to see if you can access the assigned profile.

If you (the administrator) can be successfully authenticated in the domains that were set up, the test process is complete, and you are ready to activate authentication on the network (see Activate Authentication on the Network).

Test Web-based authentication settings

To verify that authentication is working properly, make the following settings in the Group section of the console:

Step 1: Create an IP Group, “test”

1. Click the IP branch of the tree.
2. Select Add Group from the pop-up menu to open the Create New Group dialog box:



Fig. 5-2 Create New Group box

3. Enter **test** as the **Group Name**.
4. Enter the password in the **Password** and **Confirm Password** fields.
5. Click **OK** to add the group to the tree.

Step 2: Create a Sub-Group, “workstation”

1. Select the IP Group from the tree.
2. Click Add Sub Group in the pop-up menu to open the Create Sub Group dialog box:

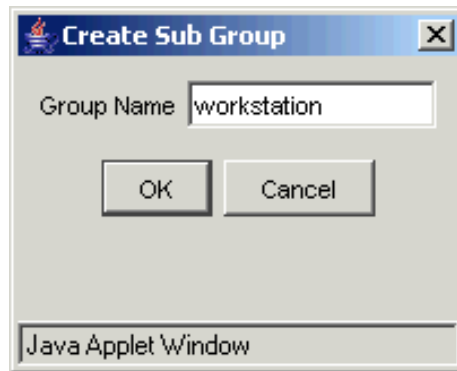


Fig. 5-3 Create Sub Group box

3. Enter ***workstation*** as the **Group Name**.
4. Click **OK** to add the Sub-Group to the IP Group.

Step 3: Set up “test” with a 32-bit net mask

1. Select the IP Group named “test” from the tree.
2. Click Members in the pop-up menu to display the Members window:

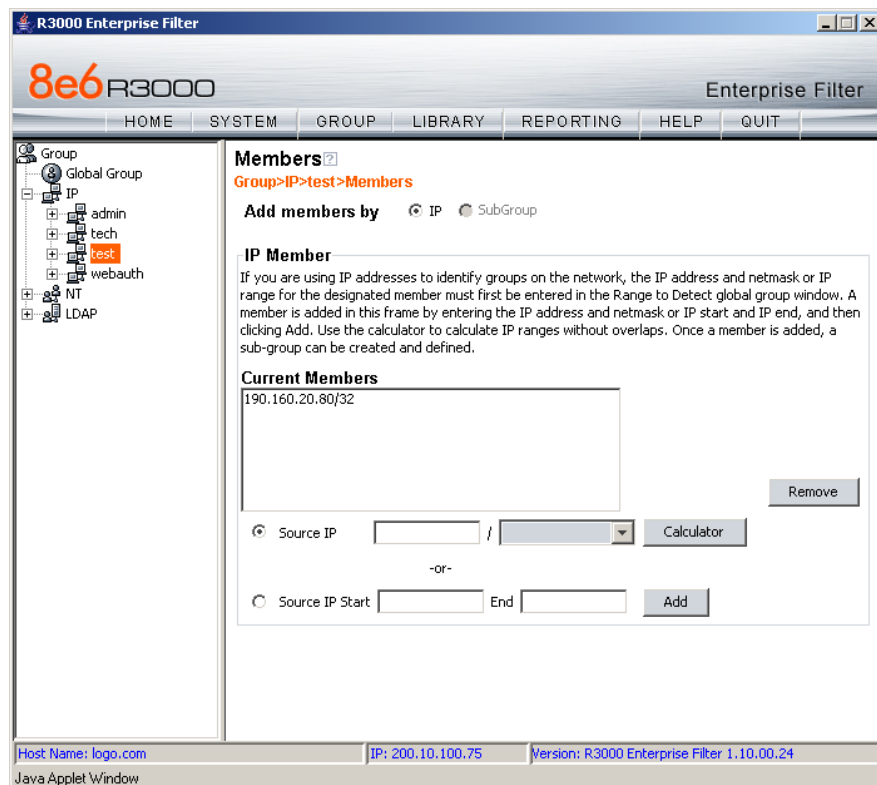


Fig. 5-4 Group Members window

3. Click the radio button corresponding to “Source IP”.
4. Enter the **Source IP** address of the workstation, and select 255.255.255.255 as the subnet mask.
5. Click **Add** to include the IP address in the Current Members list box.

Step 4: Give “workstation” a 32-bit net mask

1. Select the IP Sub-Group “workstation” from the tree.
2. Click Members in the pop-up menu to display the Members window:

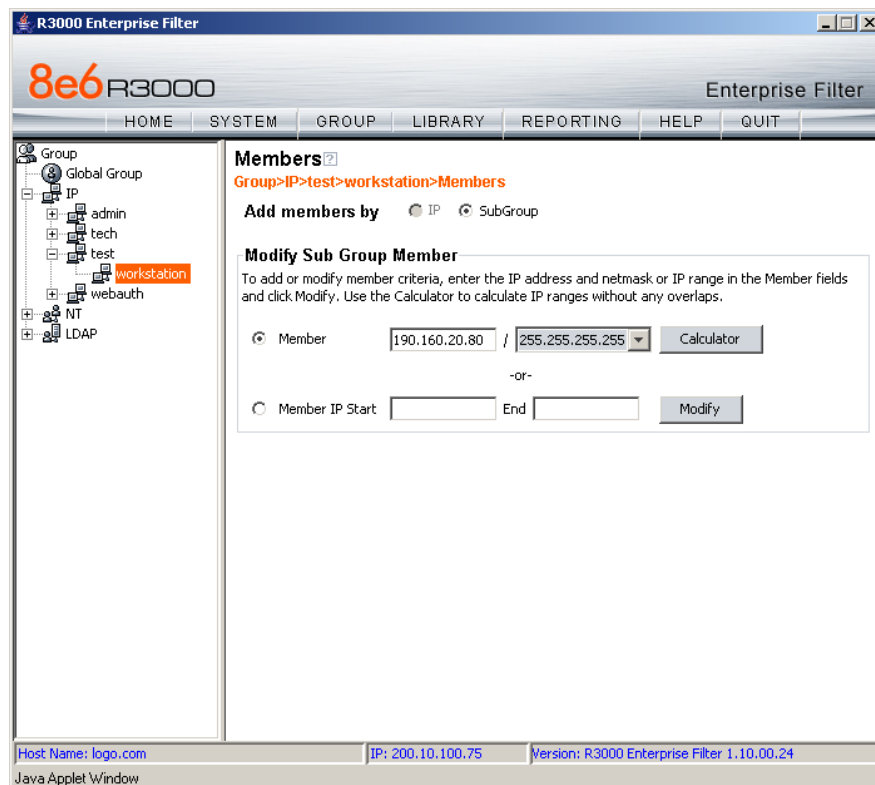


Fig. 5-5 Sub Group Members window

3. Click the radio button corresponding to “Member”.
4. In the **Member** fields, enter the IP address of the workstation, and select 255.255.255.255 as the subnet mask.
5. Click **Modify**.

Step 5: Block everything for the Sub-Group

1. Select the IP Sub-Group “workstation” from the tree.
2. Click Sub Group Profile in the pop-up menu to display the Sub Group Profile window:

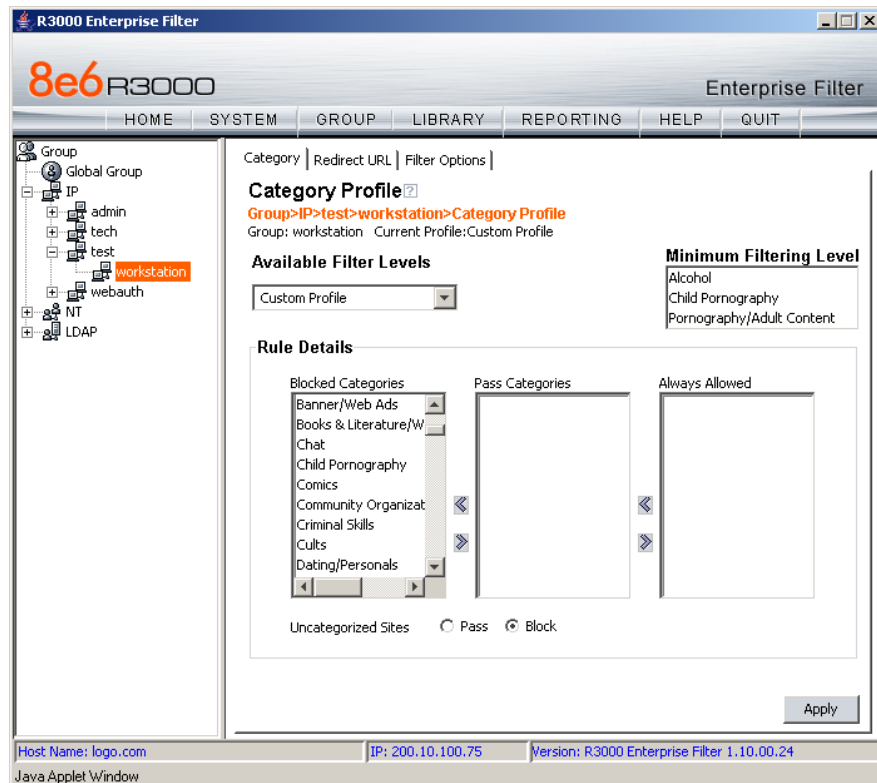


Fig. 5-6 Sub Group Profile window, Category tab

3. In the Category Profile page, move all categories to the Blocked Categories list box by selecting categories from the Pass Categories and/or Always Allowed list box(es) and using the left arrow (<) to move them to the Blocked Categories list box.



TIP: Blocks of categories can be selected by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category.

4. For **Uncategorized Sites**, click “Block”.

5. Click **Apply**.

Step 6: Use Authentication Request Page for redirect URL

1. Click the Redirect URL tab to display the Redirect URL page:

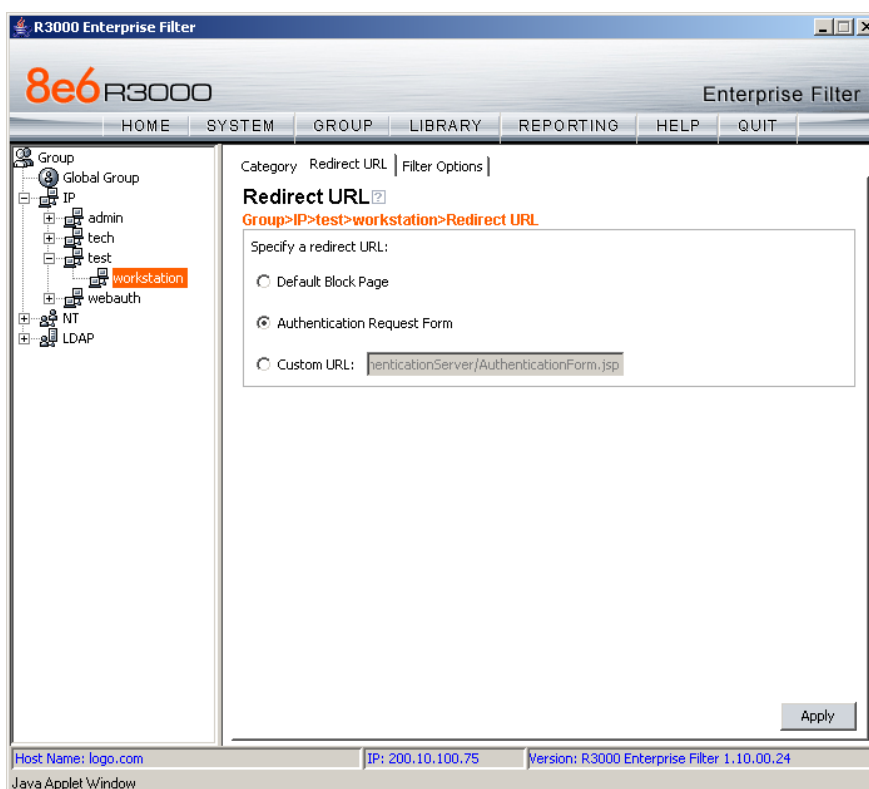


Fig. 5-7 Sub Group Profile window, Redirect URL tab

2. Select "Authentication Request Form".



NOTE: The host name of the R3000 will be used in the redirect URL of the Authentication Request Form, not the IP address. Be sure a forward/reverse DNS entry for the R3000 is made on the DNS server.

3. Click **Apply**.

Step 7: Disable filter options

1. Click the Filter Options tab to display the Filter options page:

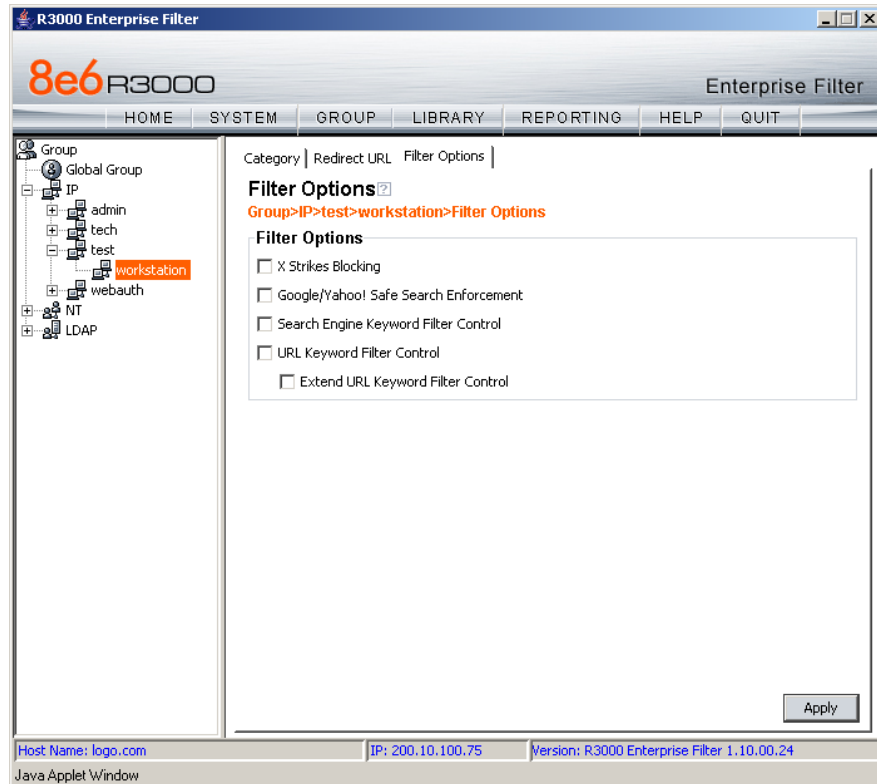


Fig. 5-8 Sub Group Profile window, Filter Options tab

2. Uncheck all the checkboxes: “X Strikes Blocking”, “Google/Yahoo! Safe Search Enforcement”, “Search Engine Keyword Filter Control”, “URL Keyword Filter Control”, and “Extend URL Keyword Filter Control”.
3. Click **Apply**.

Step 8: Attempt to access Web content



NOTE: For this step, you must have your own profile set up in order to complete the test process.

1. Launch Internet Explorer:

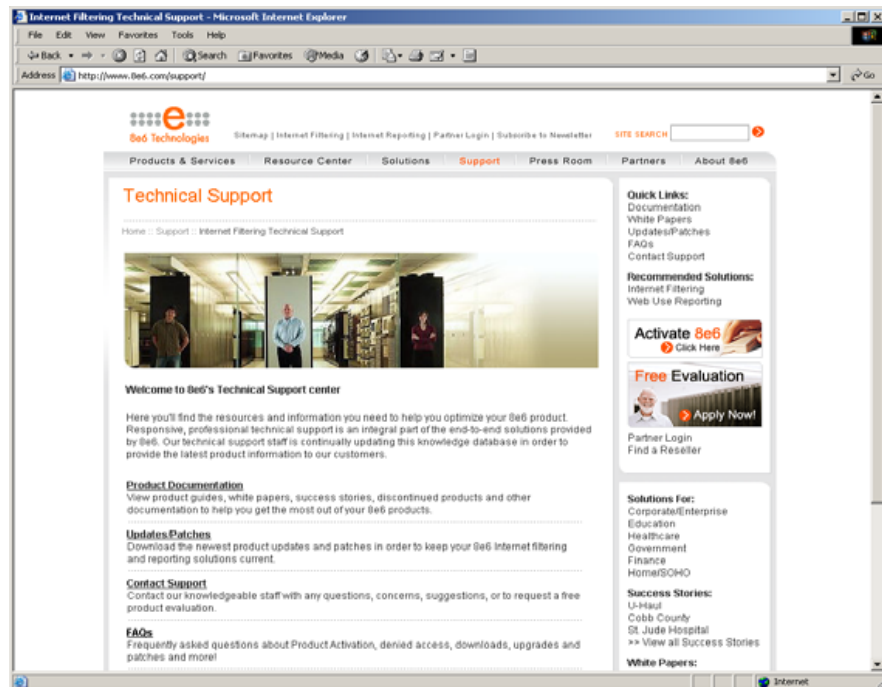


Fig. 5-9 Internet Explorer browser

2. Enter a URL in the **Address** field of the browser window.



NOTE: The URL should be one that begins with “http”—**not** “https”.

3. After clicking **Go**, the Authentication Request Form should open:

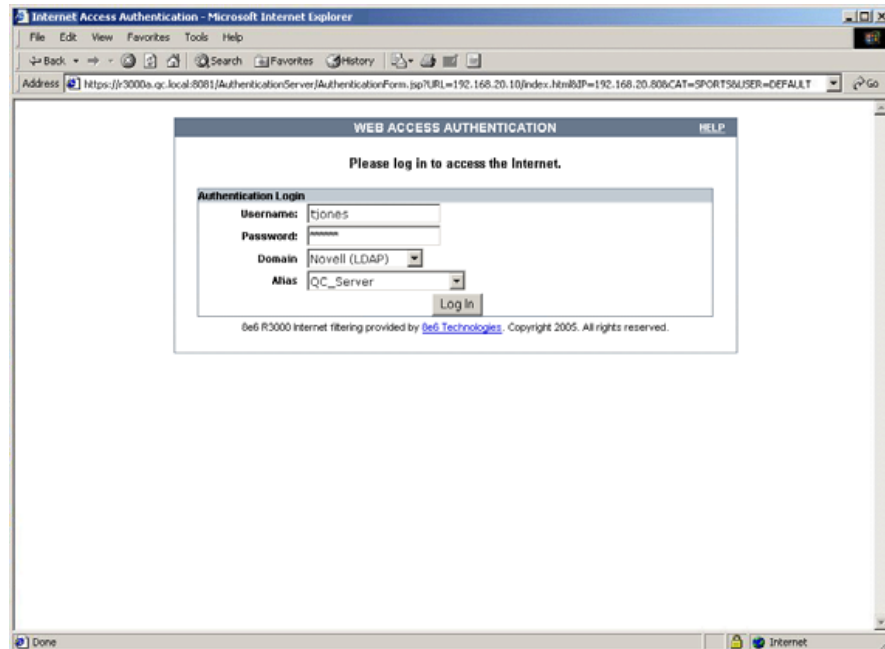


Fig. 5-10 Authentication Request Form

4. Enter the following information:

- **Username**
- **Password**

If the Domain and Alias fields display, select the following information:

- **Domain** you are using
- **Alias** name for that domain (unless “Disabled” displays and the field is greyed-out)

5. Click **Log In** to authenticate or re-authenticate yourself on the network.

The test process has been completed successfully if you are now able to access the content for the URL you entered at step 2 in this section.

Test net use based authentication settings

1. From the test workstation, go to the NET USE command line and enter the NET USE command using the following format: **NET USE \\virtualip\R3000\$**

For example: NET USE \\192.168.0.20\R3000\$

The entry you make should initiate a connection with Tier 1.



TIP: *The virtual IP address should be the same as the one entered in the Virtual IP Address to Use for Authentication field in the Authentication Settings window (see Chapter 2: Network Setup, Enter network settings for authentication).*

2. Make a Web request to a site you can access, based on your filtering profile.

The test process has been completed successfully if you are now able to access the content for the URL you entered at step 2 in this section.

Activate Authentication on the Network

After successfully testing authentication settings, you are now ready to activate authentication on the network.

To verify that authentication is ready to be activated on the network, do either of the following, based on the Tier you selected:

- **If Tier 2 or Tier 3 Web-based authentication will be used:** There are two options for Web-based authentication: IP Group authentication, and Global Group Profile authentication. Select the option you wish to use on your network. Go to the Activate Web-based authentication for an IP Group sub-section for instructions on setting up an IP Group profile for authentication. Go to the Activate Web-based authentication for the Global Group sub-section for instructions on setting up the Global Group Profile for authentication.



NOTE: *An accelerator card is recommended if using Web-based authentication.*

- **If Tier 1 net use based authentication will be used:** Go to the Activate net use based authentication sub-section for instructions on testing the login script and modifying the Global Group Profile for authenticating users.

Activate Web-based authentication for an IP Group

IP Group authentication is the preferred selection for Web-based authentication—over the Global Group Profile authentication option—as it decreases the load on the R3000.

Step 1: Create a new IP Group, “webauth”

1. Click the IP branch of the tree.
2. Select Add Group from the pop-up menu to open the Create New Group dialog box:



Fig. 5-11 Create New Group box

3. Enter **webauth** as the **Group Name**.
4. Enter the password in the **Password** and **Confirm Password** fields.
5. Click **OK** to add the group to the tree.

Step 2: Set “webauth” to cover users in range

1. Select the IP group “webauth” from the tree.
2. Click Members in the pop-up menu to display the Members window:

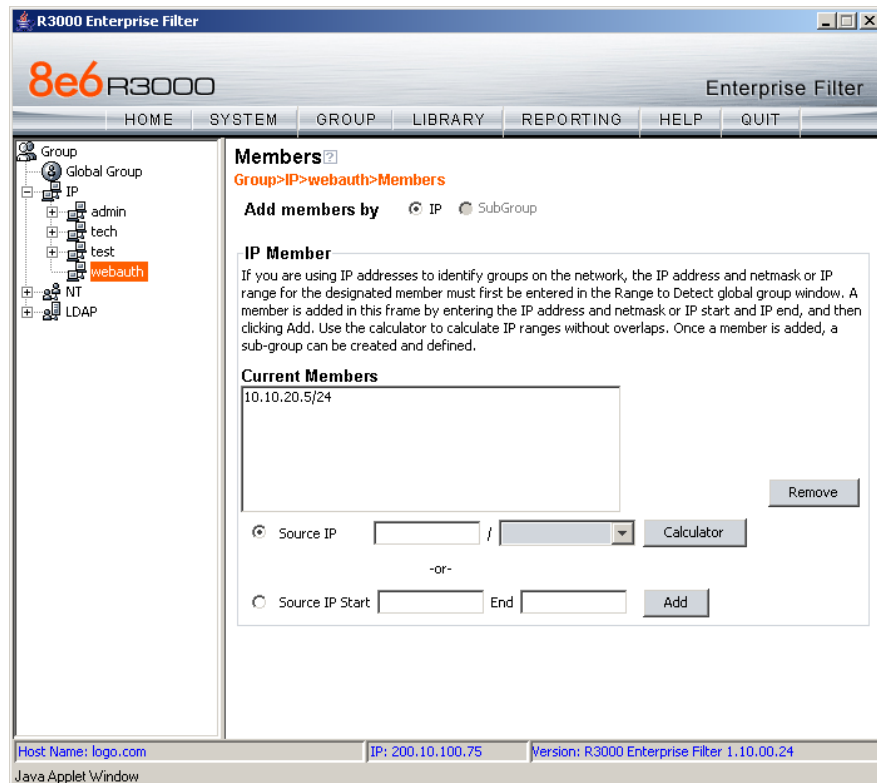


Fig. 5-12 Members window

3. Click the radio button corresponding to “Source IP”.
4. Enter the **Source IP** address of the workstation and specify the subnet mask for the range of user IP addresses of users to be authenticated.
5. Click **Add** to include the IP address range in the Current Members list box.

Step 3: Create an IP Sub-Group

1. Select the IP Group “webauth” from the tree.
2. Click Add Sub Group in the pop-up menu to open the Create Sub Group dialog box:

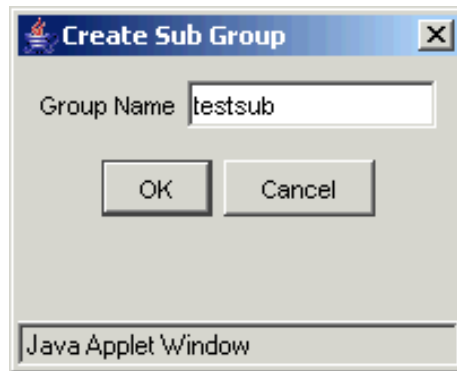


Fig. 5-13 Create Sub Group box

3. Enter the **Group Name** of your choice.
4. Click **OK** to add the Sub-Group to the IP Group.
5. Select the IP Sub-Group from the tree.
6. Click Members in the pop-up menu to display the Members window:

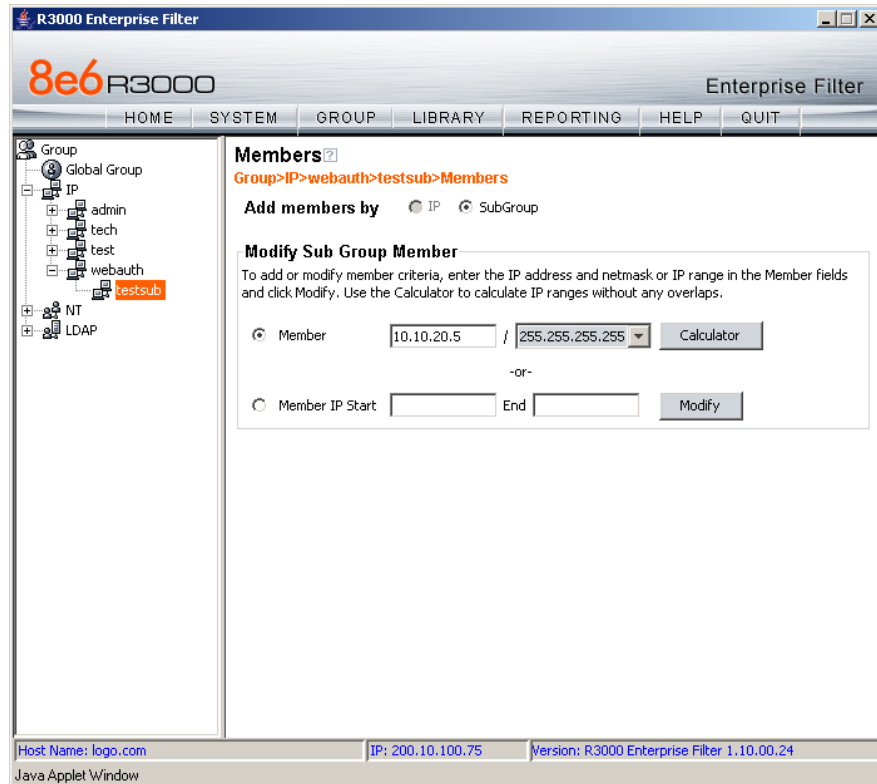


Fig. 5-14 Sub Group Members window

7. Click the radio button corresponding to “Member”.
8. In the **Member** fields, enter the IP address range for members of the Sub-Group, and specify the subnet mask.
9. Click **Modify**.

Step 4: Block everything for the Sub-Group

1. Select the IP Sub-Group from the tree.
2. Click Sub Group Profile in the pop-up menu to display the Sub Group Profile window:

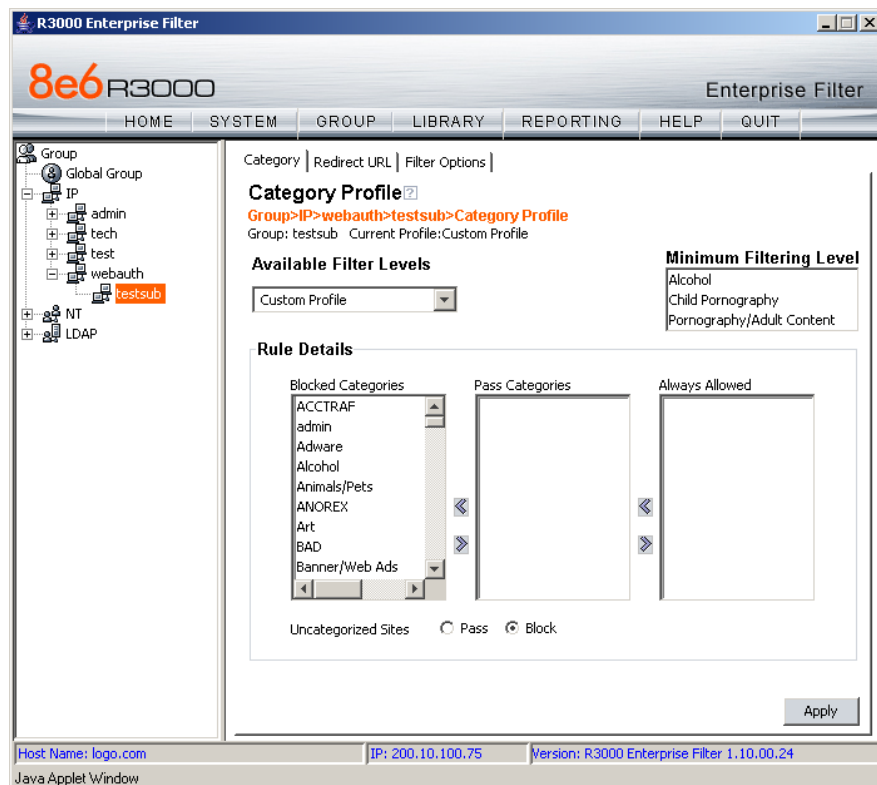


Fig. 5-15 Sub Group Profile window, Category tab

3. In the Category Profile page, move all categories to the Blocked Categories list box by selecting categories from the Pass Categories and/or Always Allowed list box(es) and using the left arrow (<) to move them to the Blocked Categories list box.



TIP: Blocks of categories can be selected by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category.

4. For **Uncategorized Sites**, click “Block”.

5. Click **Apply**.

Step 5: Use Authentication Request Page for redirect URL

1. Click the Redirect URL tab to display the Redirect URL page:

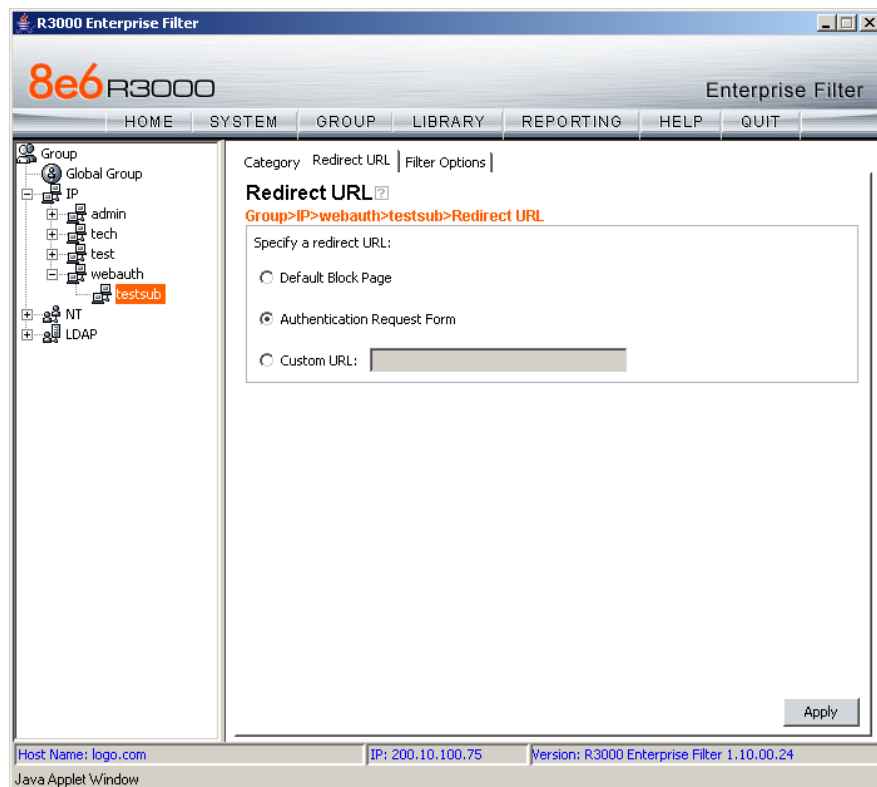


Fig. 5-16 Sub Group Profile window, Redirect URL tab

2. Select “Authentication Request Form”.



NOTE: Since the Authentication Request Form radio button selection uses the host name of the server—not the IP address—be sure there is a DNS resolution for the host name.

3. Click **Apply**.

As a result of these entries, Web-based authentication takes effect immediately, and any user in this Sub-Group will be

sent to the Authentication Request Form if he/she attempts to access content on the Internet. After filling out this form and being authenticated, the user will be able to access Internet content based on his/her filtering profile.

Step 6: Disable filter options

1. Click the Filter Options tab to display the Filter options page:

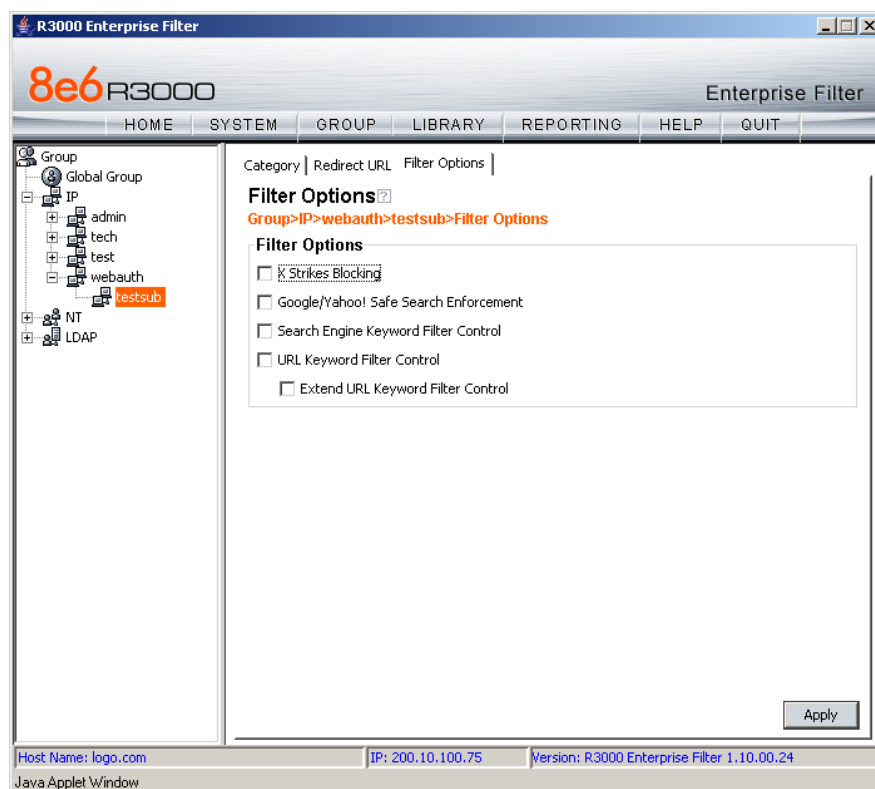


Fig. 5-17 Sub Group Profile window, Filter Options tab

2. Uncheck all the checkboxes: "X Strikes Blocking", "Google/Yahoo! Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control", and "Extend URL Keyword Filter Control".
3. Click **Apply**.

Step 7: Set Global Group to filter unknown traffic

1. Click Global Group in the tree to open the pop-up menu.
2. Select Global Group Profile to display the Category tab of the Profile window:

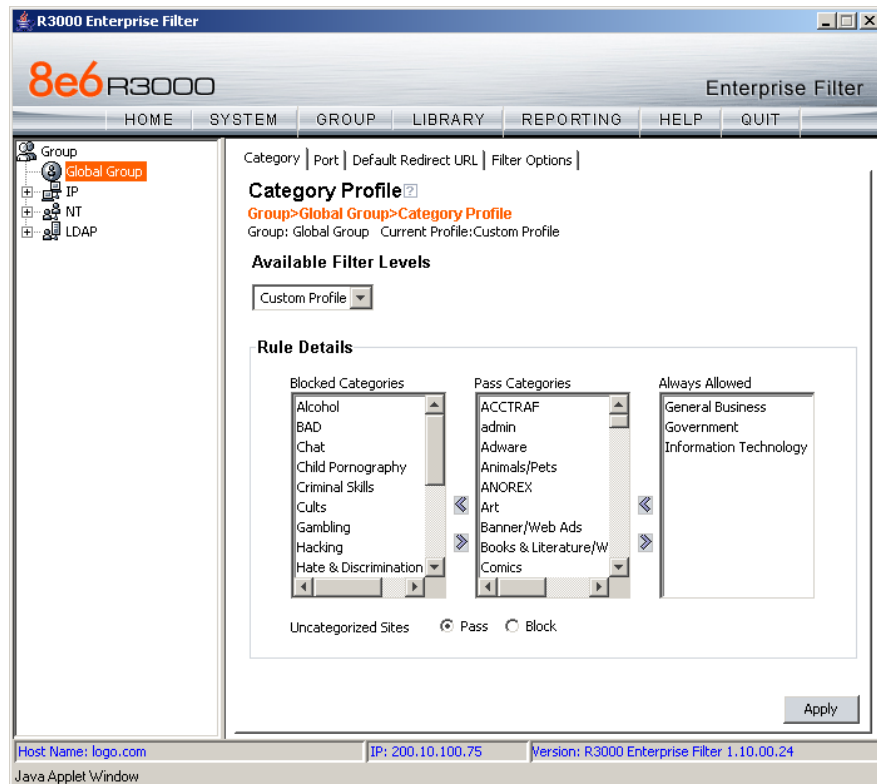


Fig. 5-18 Global Group Profile window, Category tab

- a. In the Category Profile page, select categories to block, pass, or white list, and indicate whether uncategorized sites should pass or be blocked.
 - b. Click **Apply**.
3. Click the Port tab to display the Port page:

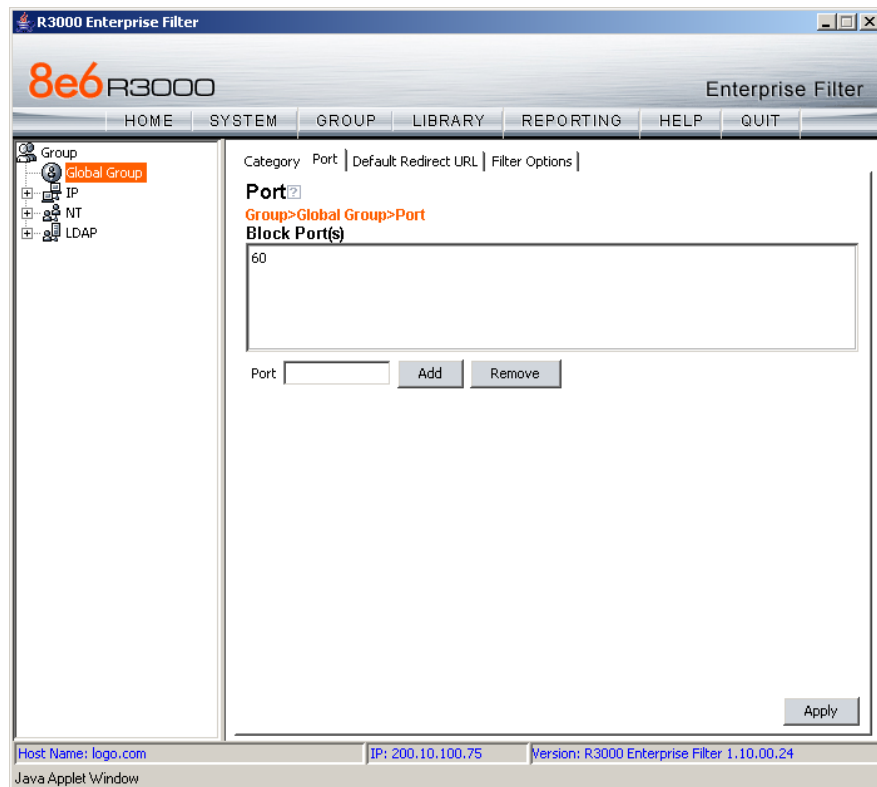


Fig. 5-19 Global Group Profile window, Port tab

- a. In the Port page, enter the **Port** number to be blocked.
- b. Click **Add** to include the port number in the Block Port(s) list box.
- c. After entering all port numbers to be blocked, click **Apply**.

4. Click the Default Redirect URL tab to display the Default Redirect URL page:

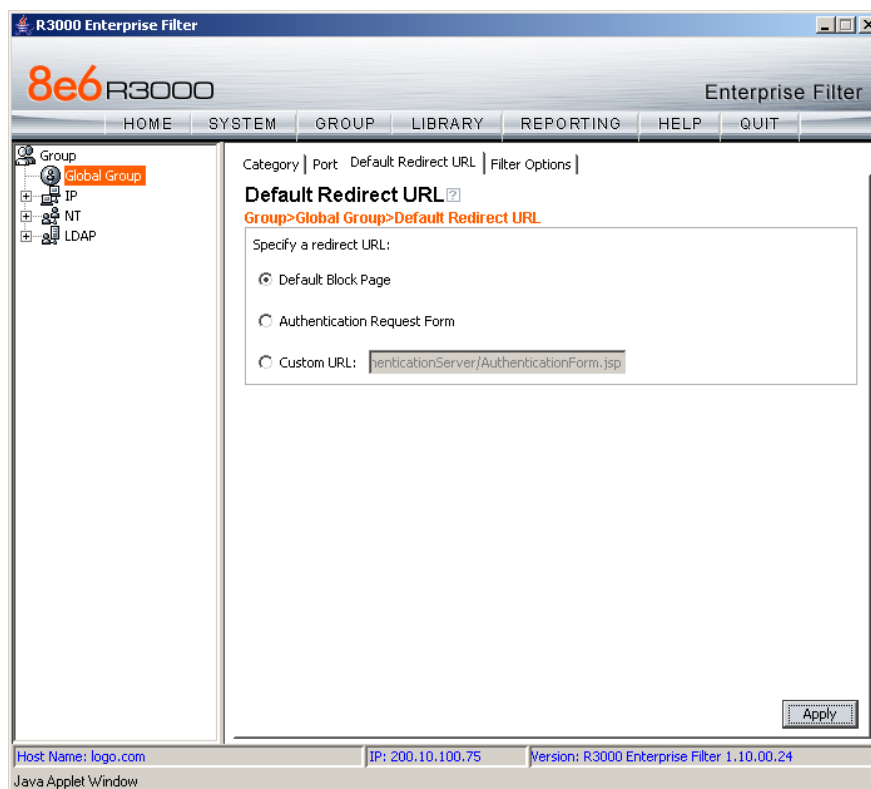


Fig. 5-20 Global Group Profile window, Default Redirect URL tab

- a. Select “Default Block Page”.
- b. Click **Apply**.

5. Click the Filter Options tab to display the Filter Options page:

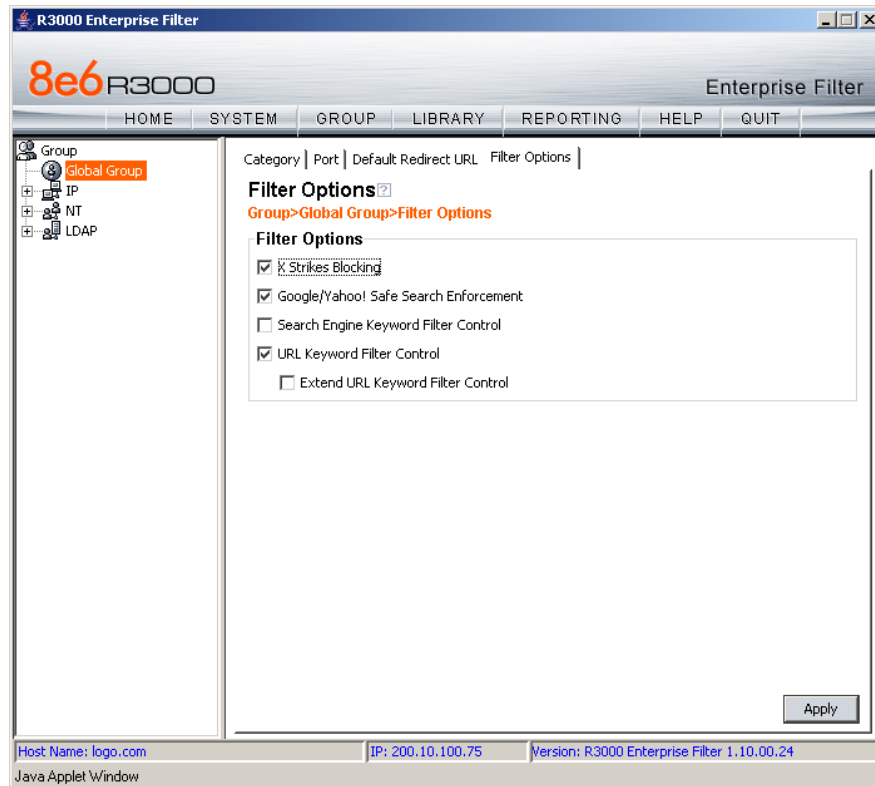


Fig. 5-21 Global Group Profile window, Filter Options tab

- a. Select filter options to be enabled.
- b. Click **Apply**.

As a result of these entries, the standard block page will display—instead of the Authentication Request Form—when any user in this Sub-Group is blocked from accessing Internet content.

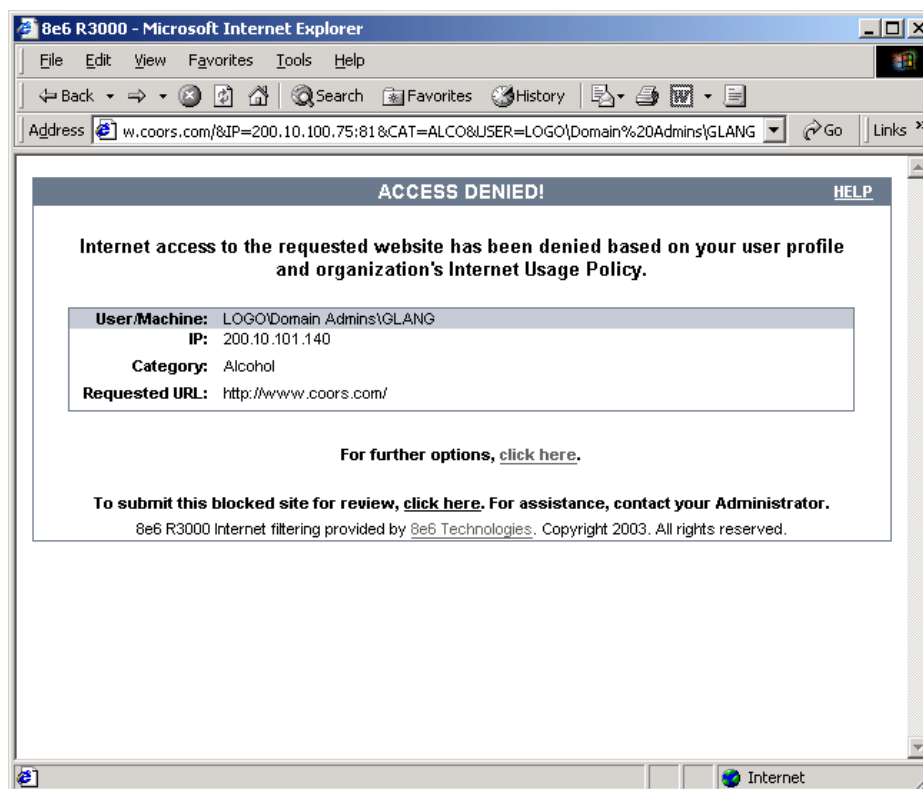


Fig. 5-22 Default Block Page

Activate Web-based authentication for the Global Group

This selection of Web-based authentication creates more of a load on the R3000 than the IP Group selection, and should only be used as an alternative to IP Group authentication.

Step 1: Exclude filtering critical equipment

This step involves the identification of equipment—such as backup servers—you wish to be excluded from being served the Authentication Request Form page.

For this step, you must choose one of two options:

- **Block Web access only** – Select this option if you do not want to log traffic for a machine that you set up to be excluded from filtering on the network. Using this option, you exclude the IP address of a machine via the Range to Detect window. If you select this option, go to Step 1A.
- **Block Web access and log traffic** – Select this option if you wish to log traffic for a machine that you set up to be excluded from filtering on the network. Using this option, you create an IP profile for the machine via the Sub Group Profile window. If you select this option, go to Step 1B.

Step 1A: Block Web access, logging via Range to Detect



NOTE: Segments of network traffic should not be defined if using the firewall mode.

Range to Detect Settings

1. Click Global Group in the tree to open the pop-up menu.
2. Select Range to Detect to display the Range to Detect Settings window:

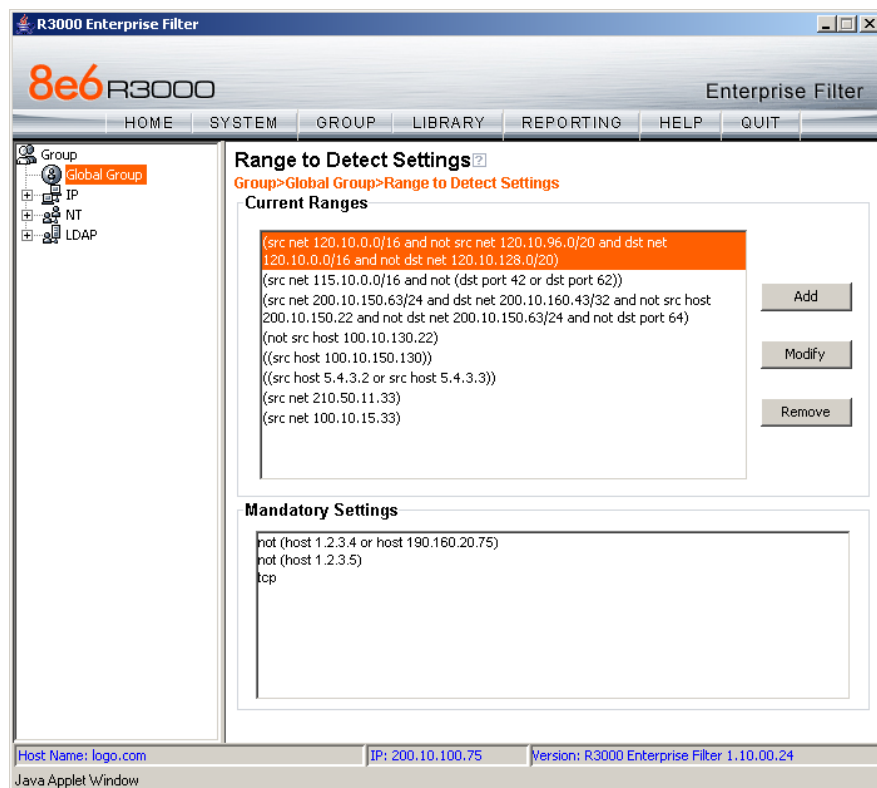


Fig. 5-23 Range to Detect Settings window, main window

3. In the Current Ranges frame, click **Add** to go to the next Settings page:

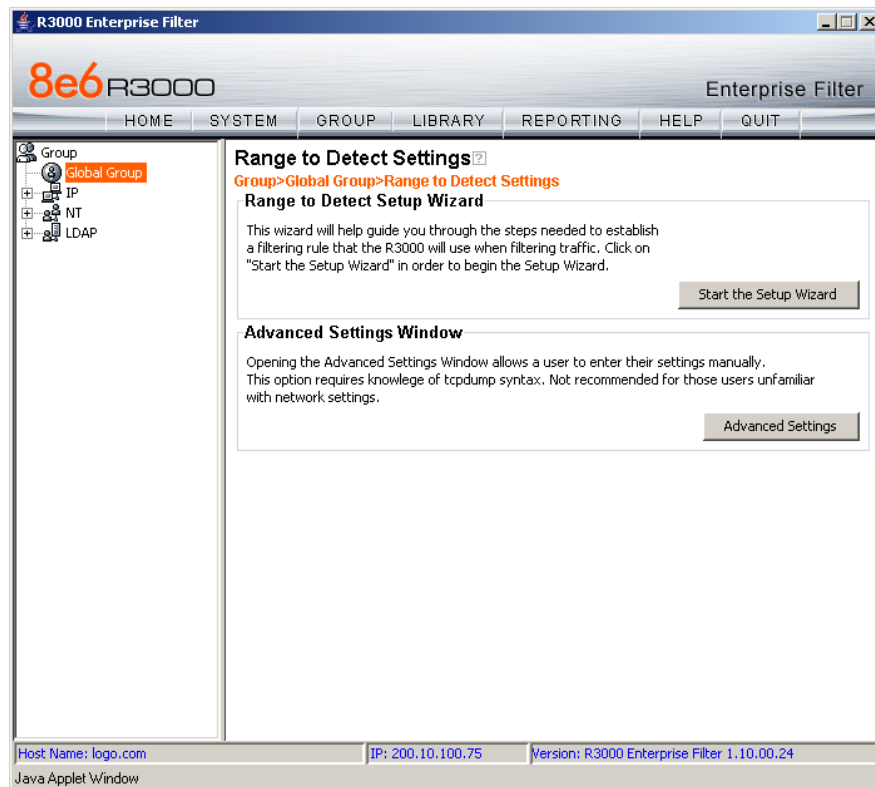


Fig. 5-24 Range to Detect Settings window, main window

4. Click **Start the Setup Wizard** to display Step 1 of the Range to Detect Setup Wizard:

Range to Detect Setup Wizard

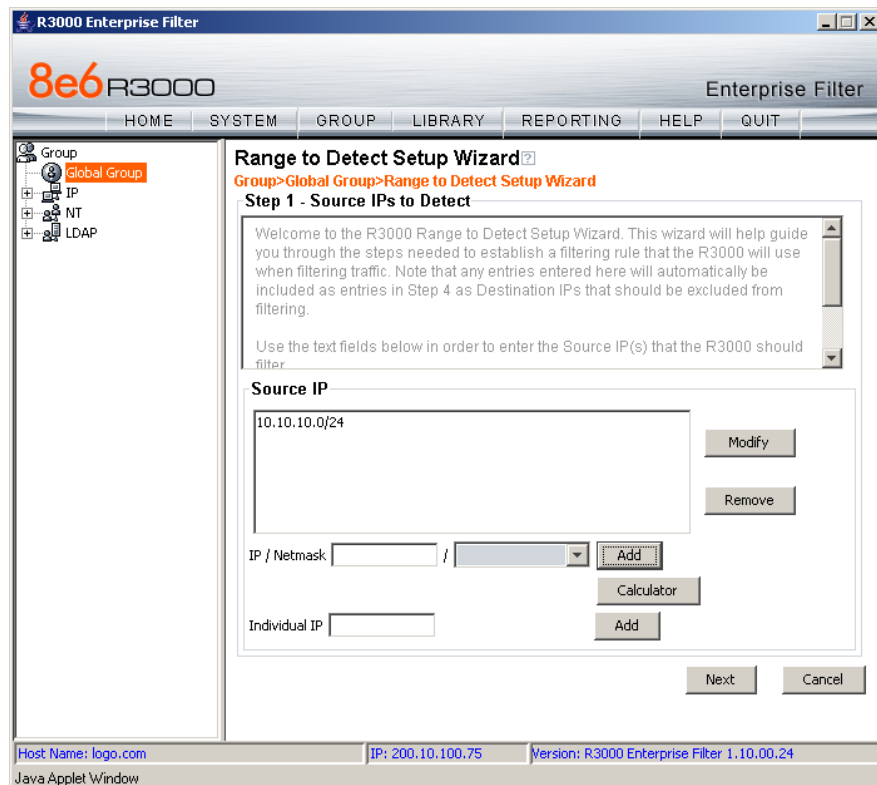


Fig. 5-25 Range to Detect Setup Wizard, Step 1

1. Enter the **IP** address and specify the **Netmask**, or enter the **Individual IP** address of the source IP address(es) to be filtered.
2. Click **Next** to go to Step 2 of the Wizard:

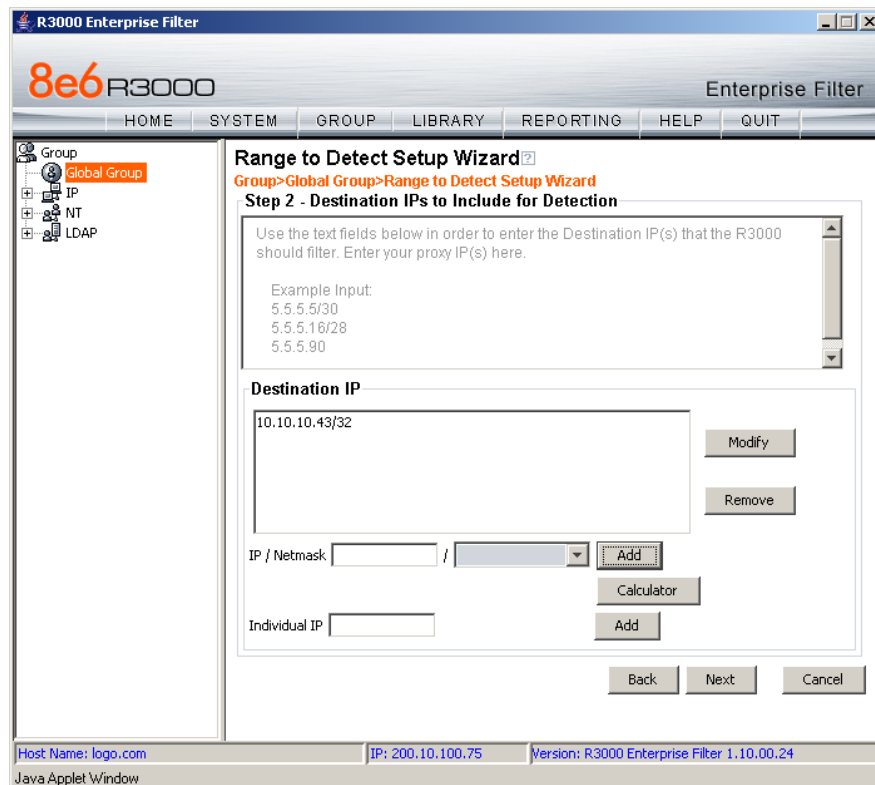


Fig. 5-26 Range to Detect Setup Wizard, Step 2

3. An entry for this step of the Wizard is optional. If there are destination IP address(es) to be filtered, enter the **IP** address and specify the **Netmask**, or enter the **Individual IP** address.
4. Click **Next** to go to Step 3 of the Wizard:

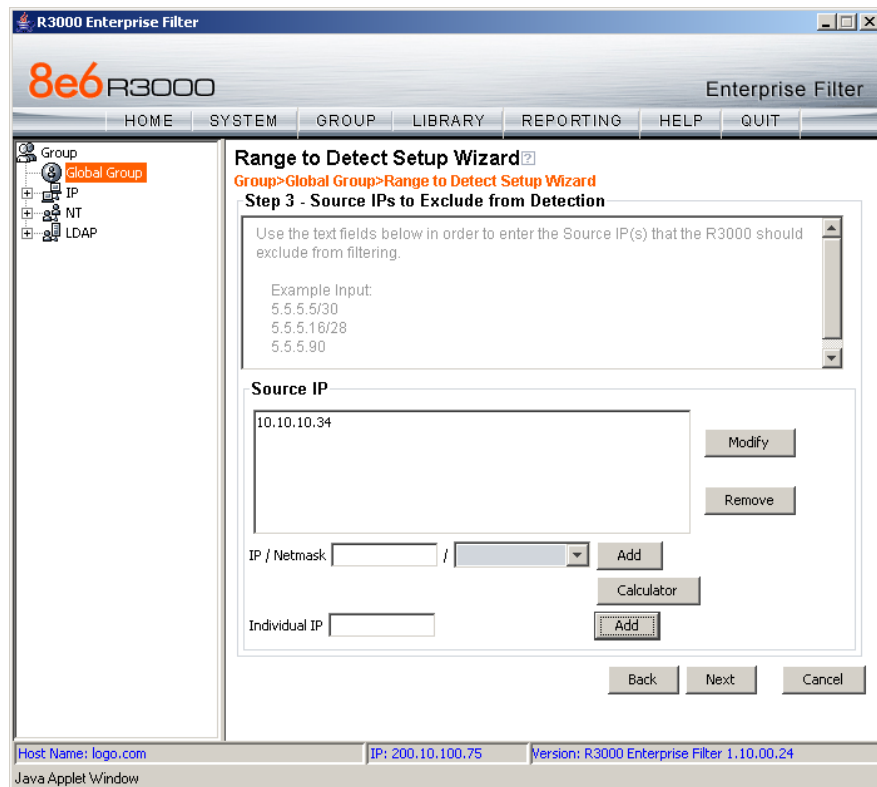


Fig. 5-27 Range to Detect Setup Wizard, Step 3

5. An entry for this step of the Wizard is optional. If there are source IP address(es) to be ignored, enter the **IP** address and specify the **Netmask**, or enter the **Individual IP** address.
6. Click **Next** to go to Step 4 of the Wizard:

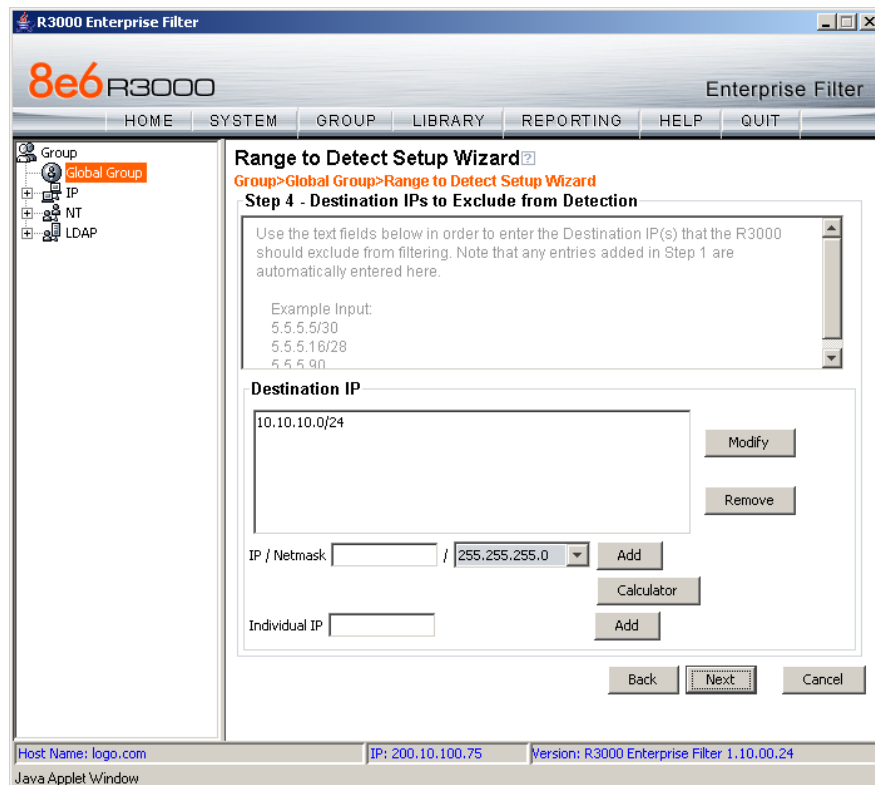


Fig. 5-28 Range to Detect Setup Wizard, Step 4

7. An entry for this step of the Wizard is optional. If there are destination IP address(es) to be ignored, enter the **IP** address and specify the **Netmask**, or enter the **Individual IP** address.
8. Click **Next** to go to Step 5 of the Wizard:

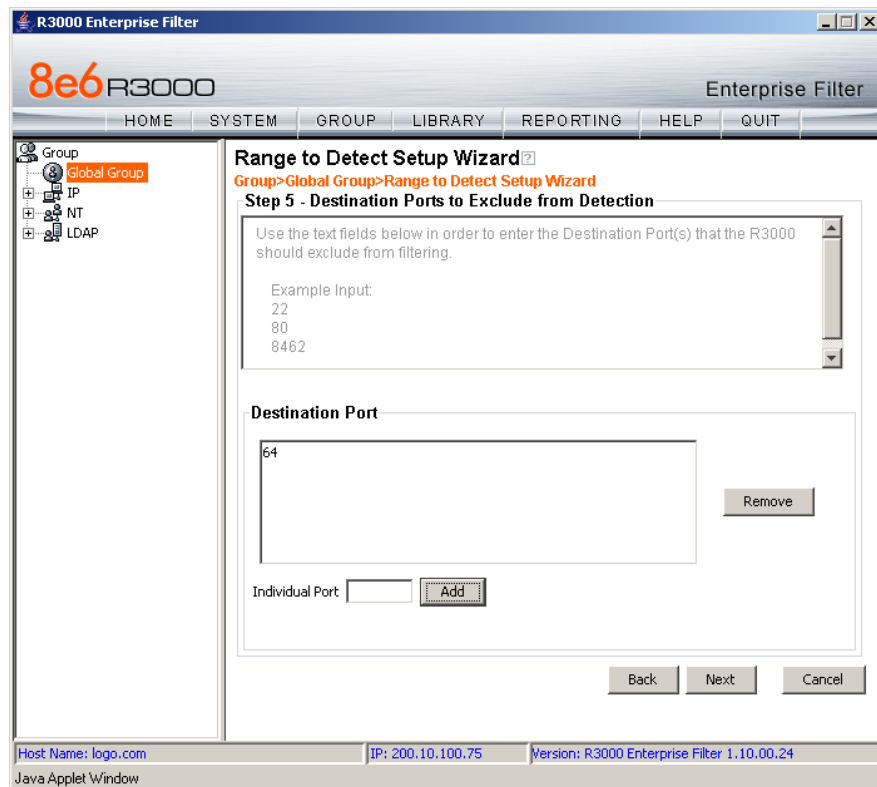


Fig. 5-29 Range to Detect Setup Wizard, Step 5

9. An entry for this step of the Wizard is optional. If there are ports to be excluded from filtering, enter each port number in the **Individual Port** field, and click **Add**.
10. Click **Next** to go to the final step of the Wizard:

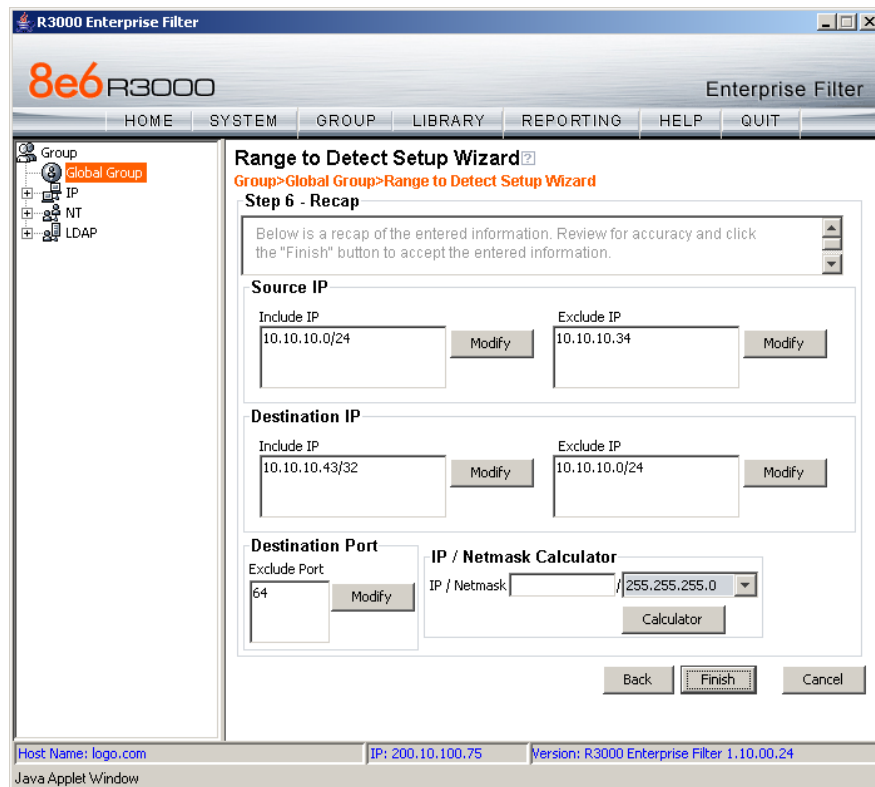


Fig. 5-30 Range to Detect Setup Wizard, Step 6

11. After review the contents in all list boxes, click **Finish** to accept all your entries.

As a result of these entries, the IP address(es) specified to be excluded will not be logged or filtered on the network.

Bypass Step 1B and go on to Step 2 to complete this process.

Step 1B: Block Web access via IP Sub-Group profile

 **NOTE:** This step assumes that the IP Group and Sub-Group have already been created.

1. Select the IP Sub-Group from the tree.
2. Click Sub Group Profile in the pop-up menu to display the Sub Group Profile window:

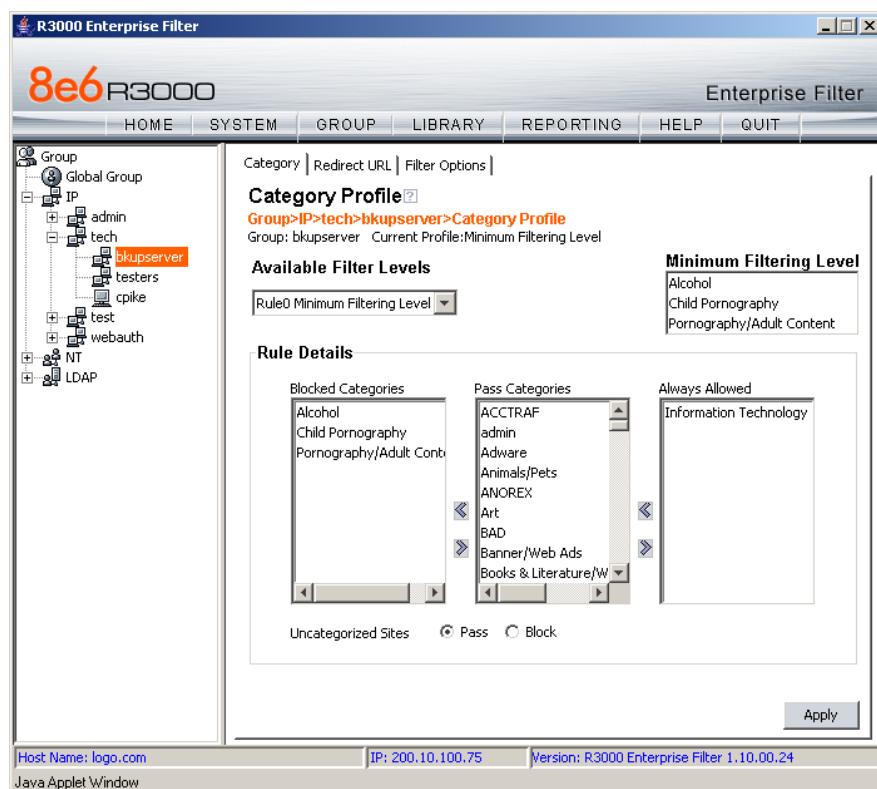


Fig. 5-31 Sub Group Profile window, Category tab

3. In the Category Profile page, create a custom profile by selecting categories to block, pass, or white list, and indicating whether uncategorized sites should pass or be blocked.
4. Click **Apply**.

5. Click the Redirect URL tab to display the Redirect URL page:

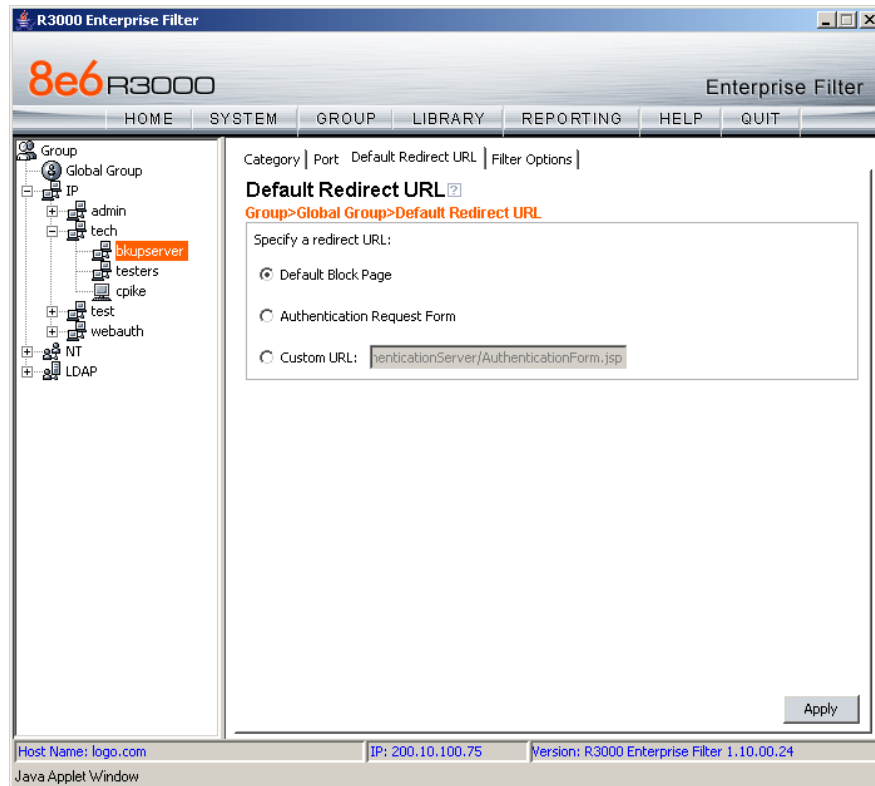


Fig. 5-32 Sub Group Profile window, Redirect URL tab

6. Select “Default Block Page”, and then click **Apply**.

7. Click the Filter Options tab to display the Filter Options page:

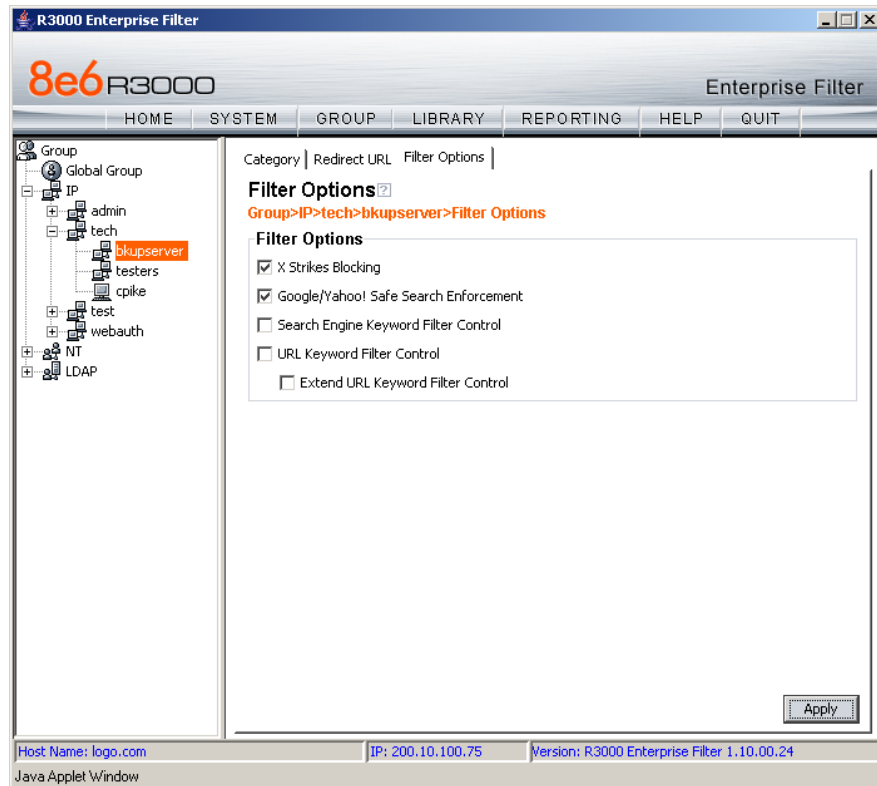


Fig. 5-33 Sub Group Profile window, Filter Options tab

8. Select filter options to be enabled, and click **Apply**.

As a result of these entries, the machine will not be served the Authentication Request Form, and will use the default block page instead.

Go on to Step 2 to complete this process.

Step 2: Modify the Global Group Profile

1. Click Global Group in the tree to open the pop-up menu.
2. Select Global Group Profile to display the Category tab of the Profile window:

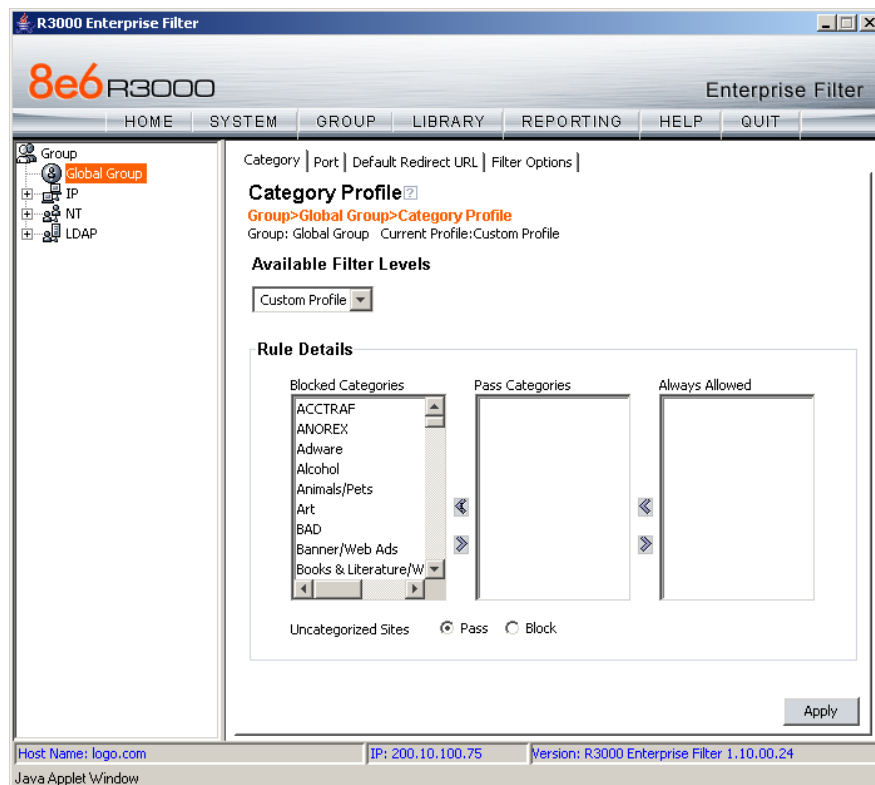
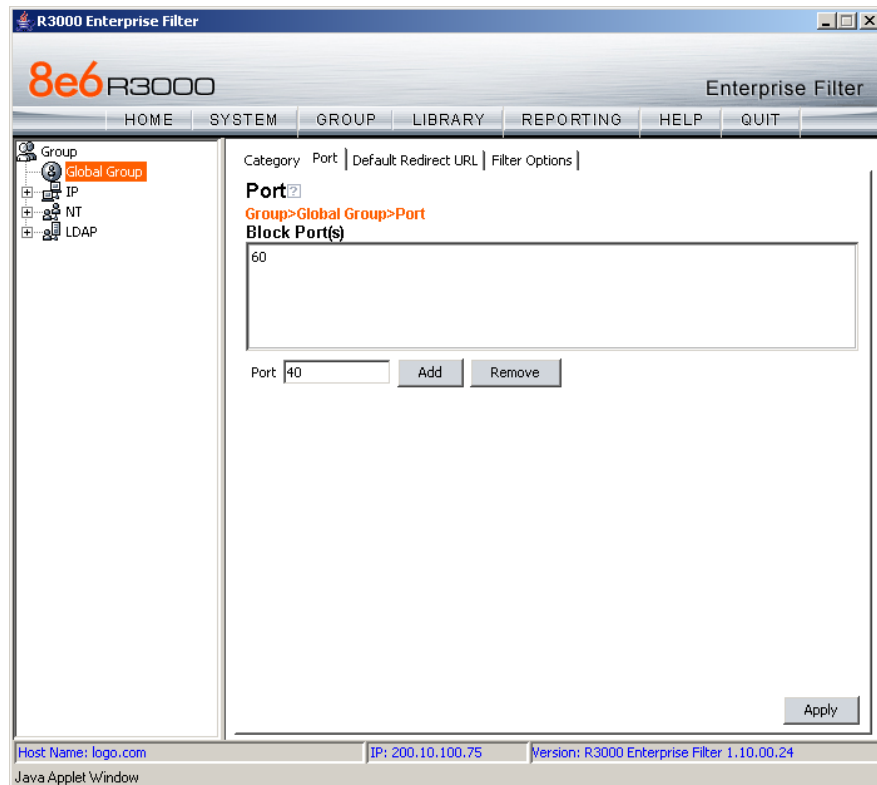


Fig. 5-34 Global Group Profile window, Category tab

- a. Block all categories and specify that uncategorized sites should be blocked.
- b. Click **Apply**.

3. Click the Port tab to display the Port page:

*Fig. 5-35 Global Group Profile window, Port tab*

- a. Enter the **Port** number to be blocked, and then click **Add** to include the port number in the Block Port(s) list box.
- b. After entering all port numbers to be blocked, click **Apply**.

4. Click the Default Redirect URL tab to display the Default Redirect URL page:

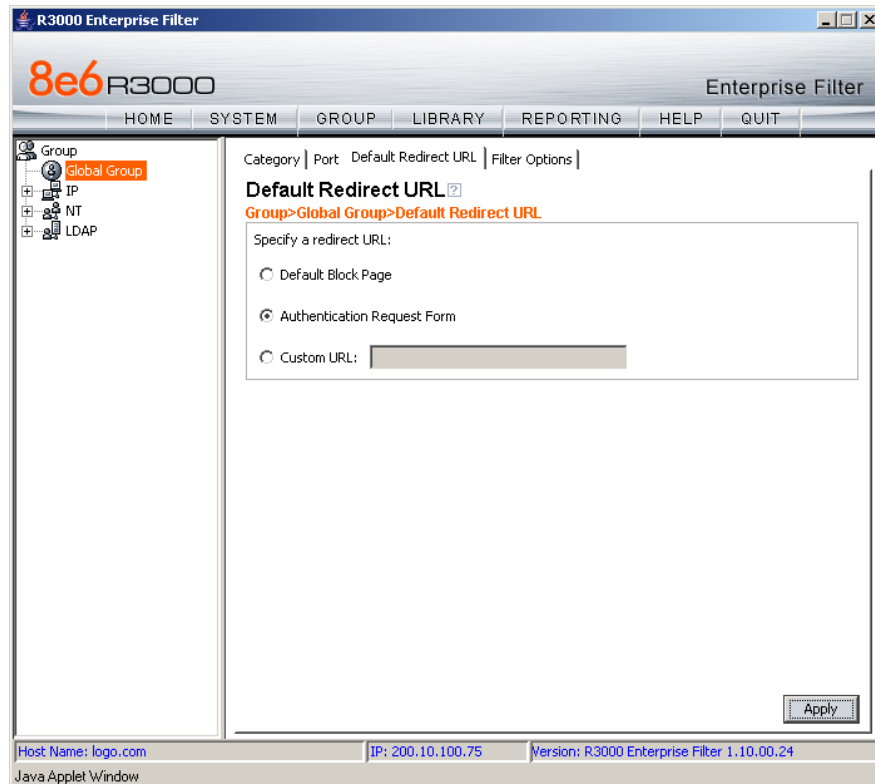


Fig. 5-36 Global Group Profile window, Redirect URL tab

- a. Select "Authentication Request Form".



NOTE: Since the Authentication Request Form radio button selection uses the host name of the server—not the IP address—be sure there is a DNS resolution for the host name.

- b. Click **Apply**.

5. Click the Filter Options tab to display the Filter Options page:

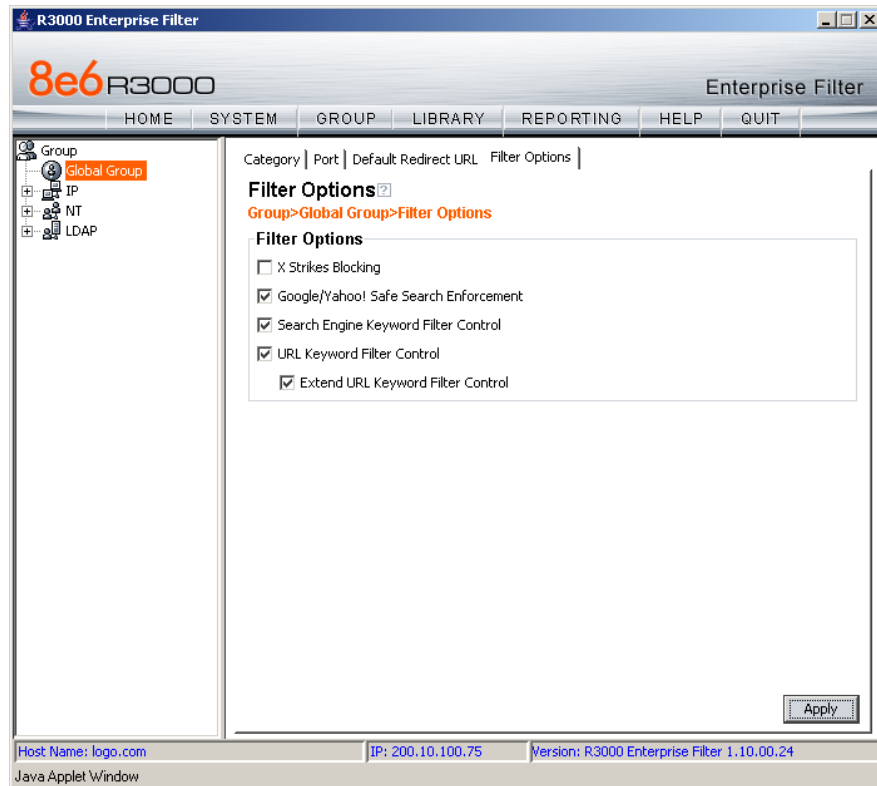


Fig. 5-37 Global Group Profile window, Filter Options tab

- a. Select filter options to be enabled.
- b. Click **Apply**.

As a result of these entries, a user who does not have a filtering profile will be served the Authentication Request Form so he/she can be authenticated.

Activate NT authentication

After testing the NET USE command, the next step is to add the NET USE command to users' login scripts. We recommend that you add the 3-try login script to the existing domain login script.

The 3-try login script is used for attempting to log in the user to the authentication server in three separate attempts, in case of a login failure.

Step 1: Modify the 3-try login script

Place a copy of the 3-try login script in the netlogon folder on your Domain Controller. Note that this sample script should be modified to use your own Virtual IP address instead of the IP address (192.168.0.20) in the sample script. This script lets users be re-authenticated from the block page without re-running the whole domain login script.

The script is as follows:

```
echo off
:start
cls
net use \\192.168.0.20\r3000$ /delete

:try1
echo "Running net use..."
net use \\192.168.0.20\r3000$
if errorlevel 1 goto :try2
if errorlevel 0 echo code 0: Success
goto :end

:try2
echo Running net use...
net use \\192.168.0.20\r3000$
if errorlevel 1 goto :try3
```

```
if errorlevel 0 echo code 0: Success
goto :end

:try3
echo Running net use...
net use \\192.168.0.20\r3000$
if errorlevel 1 goto :error
if errorlevel 0 echo code 0: Success
goto :end

:error
if errorlevel 1 echo code 1: Failed!

:end
```

Once this updated login script has been added to the domain, each time users log in to Windows they will also log in to the R3000. Users will be blocked according to the profiles set up on the domain.

Step 2: Modify the Global Group Profile

The last step of the activation process is to adjust the Global Group Profile to set the policy for members of an IP-based profile, or for users who are not authenticated.

If you set a restrictive profile, unauthenticated users will not be able to obtain access until they are successfully authenticated.

If you set up a less restrictive profile to allow access, a user can still be authenticated, but won't be prompted to authenticate him/herself unless attempting to access a site that is blocked. Since the login script will automatically run when the user logs in, a less restrictive profile might be used to allow logging with the user's name without forced blocking.

1. Click Global Group in the tree to open the pop-up menu.
2. Select Global Group Profile to display the Category tab of the Profile window.
3. In the Category Profile page, select categories to block, pass, or white list, and indicate whether uncategorized sites should pass or be blocked.
4. Click **Apply**.
5. Click the Port tab to display the Port page.
6. Enter the Port number to be blocked, and then click **Add** to include the port number in the Block Port(s) list box.
7. After entering all port numbers to be blocked, click **Apply**.
8. Click the Default Redirect URL tab to display the Default Redirect URL page. Your options on this tab will vary, based on whether your network will be using net use based authentication only, or both Web-based and net use based authentication.
9. Click the Filter Options tab to display the Filter Options page. If necessary, select appropriate filter options to be enabled, and click **Apply**.

CHAPTER 6: TECHNICAL SUPPORT

For technical support, visit 8e6 Technologies's Technical Support Web page at <http://www.8e6.com/support/index.htm>, or contact us by phone, by e-mail, or in writing.

Hours

Regular office hours are from Monday through Friday, 8 a.m. to 5 p.m. PST.

After hours support is available for emergency issues only. Requests for assistance are routed to a senior-level technician through our forwarding service.

Contact Information

Domestic (United States)

1. Call **1-888-786-7999**
2. Select *option 2*

International

1. Call **+1-714-282-6111**
2. Select *option 2*

E-Mail

For non-emergency assistance, e-mail us at **support@8e6technologies.com**

Office Locations and Phone Numbers

8e6 Corporate Headquarters (USA)

828 West Taft Avenue
Orange, CA 92865-4232
USA

Local	:	714.282.6111
Fax	:	714.282.6116
Domestic US	:	1.888.786.7999
International	:	+1.714.282.6111

8e6 Taiwan

RM B2, 13F, No. 49, Sec. 3, Minsheng E. Rd.
Taipei 104
Taiwan, R.O.C.

Taipei Local	:	2501-5285
Fax	:	2501-5316
Domestic Taiwan	:	02-2501-5285
International	:	886-2-2501-5285

8e6 China

Beijing Room 909, 9 Floor
Tower 1, Bright China Chang An Building
No. 7, Jian Guo Men Nei Dajie
Beijing 100005, China

Beijing Local	:	65180088
Fax	:	65180328
Domestic China	:	010-65180088
International	:	86-10-65180088

Support Procedures

When you contact our technical support department:

- You will be greeted by a technical professional who will request the details of the problem and attempt to resolve the issue directly.
- If your issue needs to be escalated, you will be given a ticket number for reference, and a senior-level technician will contact you to resolve the issue.
- If your issue requires immediate attention, such as your network traffic being affected or all blocked sites being passed, you will be contacted by a senior-level technician within one hour.
- Your trouble ticket will not be closed until your permission is confirmed.

APPENDIX A

User/Group File Format and Rules

The file with user/group profiles you upload to the server must be set up in a specified format, with one complete user/group profile per line. The format for the file will differ depending on whether the file contains a list of user or group profiles for an NT or LDAP server.

Each filtering profile in the file must contain the following items:

1. The username or group name.
2. Filtering profile criteria:
 - Rule number (Rule0, Rule1, etc.), or
 - rule criteria:
 - a. Ports to Block or Filter
 - b. Categories to Block or Open
 - c. Filter Mode
3. Redirect URL (optional).
4. Filter Options (optional). A zero should be placed at the end of a profile string with all filter options disabled.

Username Formats



NOTE: For examples of valid username entries, see *File Format: Rules and Examples* in this appendix, or go to ***http://www.8e6.com/r3000help/files/2group_textfile_user.html***

Rule Criteria

Rule criteria consists of selections made from the following lists of codes that are used in profile strings:

- **Port command codes:**

- A = Filter all ports
- B = Filter the defined port number(s)
- I = Open all ports
- J = Open the defined port number(s)
- Q = Block all ports
- R = Block the defined port number(s)

- **Port Numbers:**

- 21 = FTP (File Transfer Protocol)
- 80 = HTTP (Hyper Text Transfer Protocol)
- 119 = NNTP (Network News Transfer Protocol)
- 443 = HTTPS (Secured HTTP Transmission)
- Other

- **Filter Mode Values:**

- 1 = Default, Block Mode
- 2 = Monitoring Mode
- 4 = Bypassing Mode

- **Category command codes:**

- I = positioned after Category Codes designated as “blocked,” indicating that all other categories should be “open.”
- J = Open the defined category/categories
- J J = White list the defined category/categories
- Q = Block all categories
- R = Block the defined category/categories

- **Category Codes:**

For the list of category codes (short names) and their corresponding descriptions (long names), go to **http://www.8e6.com/r3000help/files/2group_textfile_cat.html#cat**



NOTE: *The list of library category codes and corresponding descriptions is subject to change due to the addition of new categories and modification of current categories. For explanations and examples of category items, go to **http://www.8e6.com/products/datab/pd_86db_r3000categories.htm***

- **Filter Option codes:**

- 0x2 = X Strikes Blocking
- 0x4 = Google/Yahoo! Safe Search
- 0x100 = Search Engine Keyword
- 0x200 = URL Keyword
- 0x1000 = Extend URL Keyword Filter Control



NOTES: *To enable multiple filter codes, add the codes together. For example, to enable all features for an NT/LDAP profile, add 2 + 4 + 100 + 200 + 1000 = 1306, which means that **0x1306** should be entered at the end of the profile string.*

*To disable all filter codes for an NT/LDAP profile, enter a **0** (zero) at the end of the profile string.*

See **http://www.8e6.com/r3000help/files/2group_textfile_format_nt.html** for examples of NT filtering profile entries, and **http://www.8e6.com/r3000help/files/2group_textfile_format_ldap.html** for examples of LDAP filtering profile entries.

File Format: Rules and Examples

When setting up the file to upload to the server, the following items must be considered:

- Each profile must be entered on a separate line in the file.
- Category Codes must be entered in capital letters.
- Port and category command codes must be entered in capital letters.
- A redirect URL cannot exceed 200 characters in length.
- The string must end with a “0” (zero) if no filter options will be enabled.

NT User List Format and Rules

When setting up the “ntuserprofile.conf” file, each entry must consist of the username, and either a rule number or rule criteria (port, category, and filter mode specifications). A redirect URL can be included, if a specific URL should be used in place of the standard block page. If a redirect URL is not included, a blank space should be entered in its place in the profile string. Segments of the profile string should be separated by commas (,). A zero (0) should be placed at the end of a profile string without any filter options enabled.

**JSmith, B 80 R 21 ,J J FINAN Q, 1, http://
www.8e6.com,0
John_Doe, Q, R AUTO GENTER I, 1, ,0x104
Doe-Jane, Rule1, , 0x202**

When translated, these strings of code mean:

- NT profile for a user with ID “JSmith”: Filter port 80, Block port 21, White List and Open Financial Category and Block all other categories, use filter mode 1, use redirect URL <http://www.8e6.com> in place of the standard block page, all filter options disabled.
- NT profile for a user with ID “John_Doe”: Block all ports, Block Automobile and Entertainment categories, use filter mode 1, Google/Yahoo! Safe Search and Search Engine Keyword filter options enabled.
- NT profile for a user with ID “Doe-Jane”: Bypass all categories, use standard block page, X Strikes Blocking and URL Keyword filter options enabled.

NT Group List Format and Rules

When setting up the “ntgroupprofile.conf” file, each entry must consist of the group name, and either a rule number or rule criteria (port, category, and filter mode specifications). A redirect URL can be included, if a specific URL should be used in place of the standard block page. If a redirect URL is not included, a blank space should be entered in its place in the profile string. Segments of the profile string should be separated by commas (,). A zero (0) should be placed at the end of a profile string without any filter options enabled.

Admin, Rule1, http://www.cnn.com, ,0x4
Sales, Rule2, ,0x300
Tech, A, R CHAT KDPO RN FINAN GGAMES
GPORN I, 1, , 0x6

When translated, these strings of code mean:

- NT profile for a group with ID “Admin”: Bypass all categories, use redirect URL <http://www.cnn.com> in place of the standard block page, Google/Yahoo! Safe Search filter option enabled.
- NT profile for a group with ID “Sales”: Block Porn category, use standard block page, Search Engine Keyword and URL Keyword filter options enabled.
- NT profile for a group with ID “Tech”: Filter all ports, Block Chat, Child Porn, Finance, and Games categories, but leave all other categories open, use filter mode 1, use standard block page, X Strikes Blocking and Google/Yahoo! Safe Search filter options enabled.

LDAP User List Format and Rules

When setting up the “ldapuserprofile.conf” file, each entry must consist of the Distinguished Name (DN), with each part of the DN separated by commas (.). The DN should be followed by a semicolon (;), and then a rule number or rule criteria (port, category, and filter mode specifications). A redirect URL can be included, if a specific URL should be used in place of the standard block page. If a redirect URL is not included, a blank space should be entered in its place in the profile string. Each segment of the profile string following the semicolon for the DN should be separated by commas (.). A zero (0) should be placed at the end of a profile string without any filter options enabled. For example:

**CN=Jane Doe, CN=Users, DC=qc, DC=local; R 21 A, J
J FINAN Q, 1, http://www.cnn.com, 0x2
CN=Public\, Joe Q., OU=Users, OU=Sales, DC=qc,
DC=local; Q, R AUTO GENTER I, 1, ,0x4**



NOTE: The DN format must contain the username and user group “CN” (“common name”) attribute type, and the domain and DNS suffix “DC” (“domain component”) attribute type. The “OU” (“organizational unit”) attribute type also can be included. Each attribute type should be followed by an equals sign (=), and separated by a comma (.).

When translated, these strings of code mean:

- LDAP profile for a user with username “Jane Doe”, user group “Users”, domain “qc”, DNS suffix “.local”: Block port 21 and Filter all other ports, White List and Open Financial Category and Block all other categories, use filter mode 1, use redirect URL <http://www.cnn.com> in place of the standard block page, X Strikes Blocking filter option enabled.

- LDAP profile for a user with username “Public\, Joe Q.”, organizational units “Users” and “Sales”, domain “qc”, DNS suffix “.local”: Block all ports, Block Automobile and Entertainment categories, use filter mode 1, use standard block page, Google/Yahoo! Safe Search filter option enabled.

LDAP Group List Format and Rules

When setting up the “ldapgroupprofile.conf” file, each entry must consist of the Distinguished Name (DN), with each part of the DN separated by commas (,). The DN should be followed by a semicolon (;), and then a rule number or rule criteria (port, category, and filter mode specifications). A redirect URL can be included, if a specific URL should be used in place of the standard block page. If a redirect URL is not included, a blank space should be entered in its place in the profile string. Each segment of the profile string following the semicolon for the DN should be separated by commas (,). A zero (0) should be placed at the end of a profile string without any filter options enabled. For example:

CN=Sales, CN=Users, DC=qc, DC=local; Rule1, 1, http://www.cnn.com, 0x102



NOTE: The DN format must contain the group name—and, if applicable—user group “CN” (“common name”) attribute type, and the domain and DNS suffix “DC” (“domain component”) attribute type. The “OU” (“organizational unit”) attribute type also can be included. Each attribute type should be followed by an equals sign (=), and separated by a comma (,).

When translated, this string of code means:

- LDAP profile for group with ID “Sales”, user group “Users”, domain “qc”, DNS suffix “.local”: Bypass all categories, use filter mode 1, use redirect URL http://www.cnn.com in place of the standard block page, X Strikes Blocking and Search Engine Keyword filter options enabled.

APPENDIX B

Ports for Authentication System Access

The following ports should be used for authentication system access:

Type	No.	Function
TCP	8081	Used between the R3000's transmitting interface and the SSL block page for Tier 2 or Tier 3 authentication.
TCP	836	Used between the R3000's Virtual IP address and Java applet for Tier 3 authentication.
TCP	139	Used between the R3000 and workstations requiring Tier 1 or Tier 3 authentication.
TCP/ UDP	137	Used between the R3000 and workstations requiring Tier 1 authentication.
LDAP	389	Used for communicating with domain controllers in order to bind with them so that user/group information can be queried/accessed.
LDAPS	636	Used for communicating with domain controllers in order to bind with them so that user/group information can be queried/accessed.

APPENDIX C

LDAP Server Customizations

The R3000 has been tested on common types of standard LDAP servers with default settings. However, due to the number of LDAP servers available, and the limitless ways in which any type of LDAP server can be configured, customizations may need to be made on such an LDAP server that fits either description.



NOTE: Please contact technical support for assistance in implementing any of the changes described in this appendix.

OpenLDAP Server Scenario

Not all users returned in User/Group Browser

In this scenario, a query is performed in the LDAP User/Group Browser window on an OpenLDAP server, and not all users are returned.

To resolve this problem, do the following:

1. Change the current directory to **/usr/local/shadow/etc/ldapgroup**
2. Find the subdirectory bearing the name of the LDAP domain, and change the current directory to that subdirectory.
3. Open the file "ldapobjectdef.conf" for editing.
4. Search for the line "LDC_LDAP_query_name_prefix CN="
5. Replace "CN=" with "uid=" and save these changes.
6. Restart the R3000.

APPENDIX D

Disable SMB Signing Requirements

SMB Signing is a Windows security feature that is not currently supported by the R3000. If you are running a Windows 2000 or Windows 2003 server and are using NTLM, then you need to make SMB Signing “not required.”

SMB Signing Compatibility

To find out whether SMB Signing on your Windows server is compatible with the R3000, refer to the chart below:

Server	R3000 Auth Mode	SMB Signing Enabled	SMB Signing Disabled	SMB Signing Not Defined
Win2000 mixed	NT Tier 1, 2, 3	Not compatible	Compatible	Compatible
Win2000 native	NT Tier 1, 2, 3	Not compatible	Not compatible	Not compatible
Win2003 mixed	NT Tier 1, 2, 3	Not compatible	Compatible	Not compatible
Win2003 native	NT Tier 1, 2, 3	Not compatible	Not compatible	Not compatible
Win2000 mixed	LDAP Tier 1, 2, 3	Compatible	Compatible	Compatible
Win2000 native	LDAP Tier 1, 2, 3	Compatible	Compatible	Compatible
Win2003 mixed	LDAP Tier 1, 2, 3	Compatible	Compatible	Compatible
Win2003 native	LDAP Tier 1, 2, 3	Compatible	Compatible	Compatible

Disable SMB Signing Requirements in Windows 2003

By default, the SMB protocol in Windows 2003 is set to “Not Defined = On”. To disable (turn “Off”) SMB Signing, do the following:

1. From your Windows 2003 workstation, go to Start > All Programs > Administrative Tools > Active Directory Users and Computers:



Fig. D-1 Go to Active Directory Users and Computers

2. When the Active Directory Users and Computers window opens, click Domain Controllers in the left panel to open the pop-up menu:

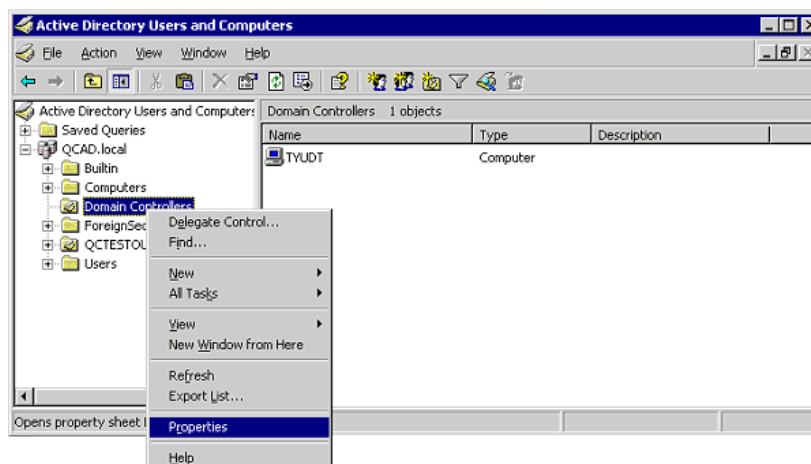


Fig. D-2 Select Properties in the Domain Controllers pop-up menu

3. Select Properties to open the Domain Controllers Properties dialog box:

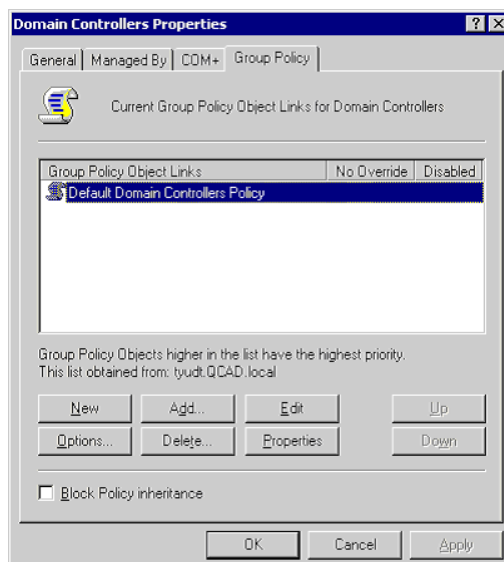


Fig. D-3 Domain Controllers Properties

4. Click the Group Policy tab, choose the Default Domain Controllers Policy, and then click **Edit** to open the Group Policy Object Editor window:

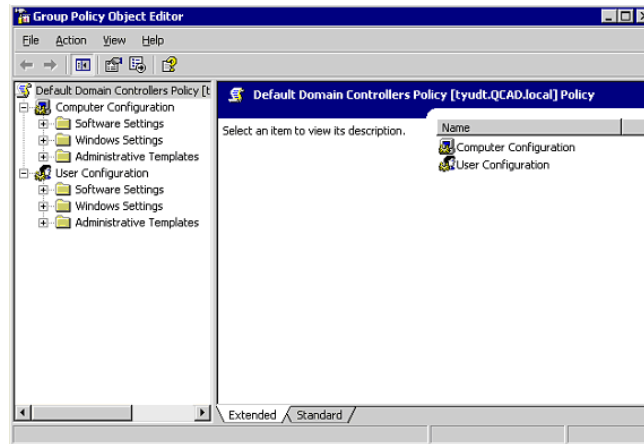


Fig. D-4 Group Policy Object Editor window

5. In the left panel, go to the Computer Configuration branch of the tree and select the Windows Settings folder to display the Windows Settings contents in the right panel:

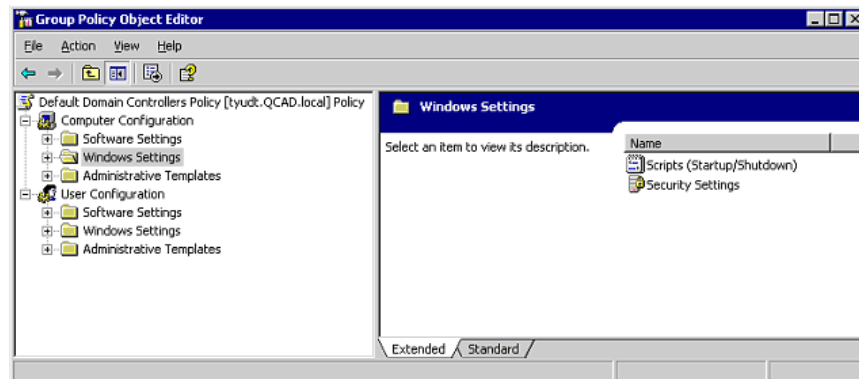


Fig. D-5 Group Policy Object Editor window, Windows Settings

6. Choose Security Settings to display the contents of this folder in the right panel:

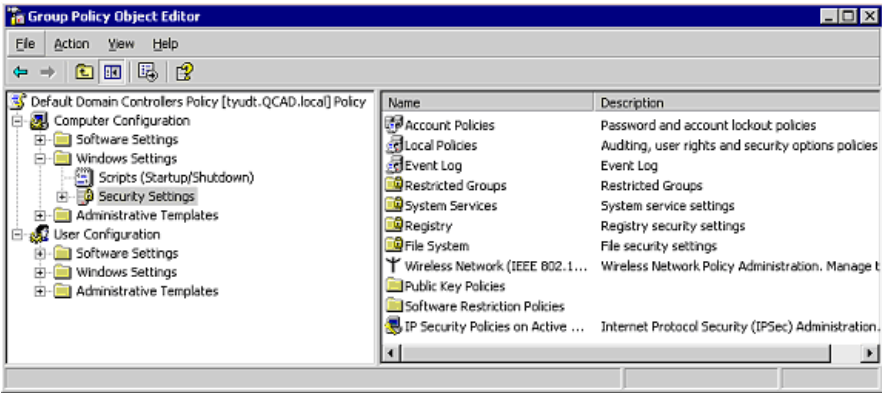


Fig. D-6 Group Policy Object Editor window, Security Settings

7. Select Local Policies to display the contents of this folder in the right panel:

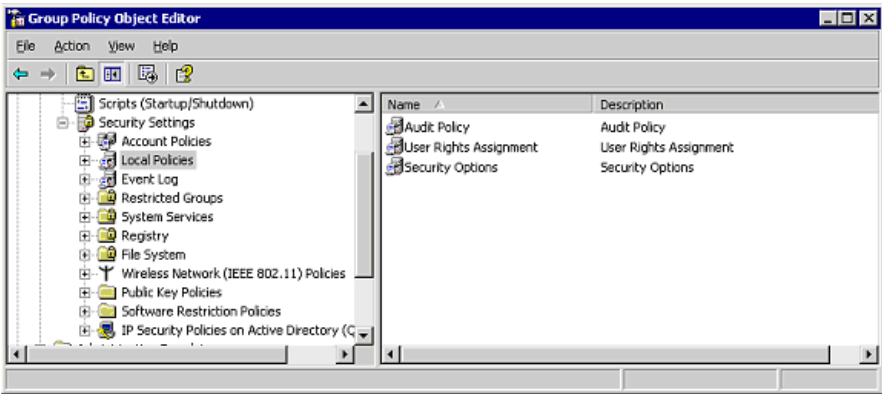


Fig. D-7 Group Policy Object Editor window, Local Policies

8. Select Security Options to display the contents of this folder in the right panel:

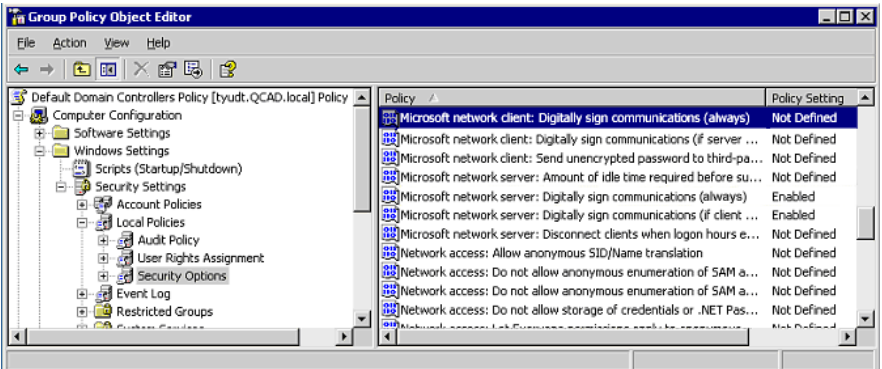


Fig. D-8 Group Policy Object Editor window, Security Options

Scroll down and find “Microsoft network client: Digitally sign communications (always)”.

9. Right-click this item to open the pop-up menu, and select Properties to open the dialog box with the Security Policy Setting tab:

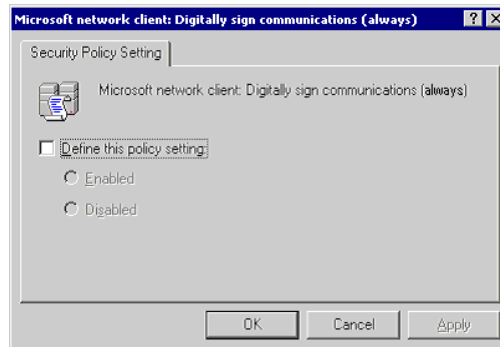


Fig. D-9 Define this policy setting

Click in the “Define this policy setting” checkbox to activate the radio buttons. Choose “Disabled”, and then click **OK**.

10. Go back to the Group Policy Object Editor window (see Fig. D-8) and find the policies for the following items:
 - Microsoft network server: Digitally sign communications (always)
 - Domain controller: LDAP server signing requirements
 - Domain controller: LDAP client signing requirementsFor each of these items, follow the instructions in step 9.

APPENDIX E

Obtain or Export an SSL Certificate

When using Web-based authentication, the LDAP server's SSL certificate needs to be exported and saved to the hard drive, then uploaded to the R3000 so that the R3000 will recognize LDAP server as a trusted source.

This appendix provides steps on exporting an SSL certificate from a Microsoft Active Directory or Novell server—the most common types of LDAP servers. Also included is information on obtaining a Sun ONE server's SSL certificate.

Export an Active Directory SSL Certificate

Verify certificate authority has been installed

1. From the console of the LDAP server, go to Start > Programs > Administrative Tools > Certification Authority to open the Certification Authority window:

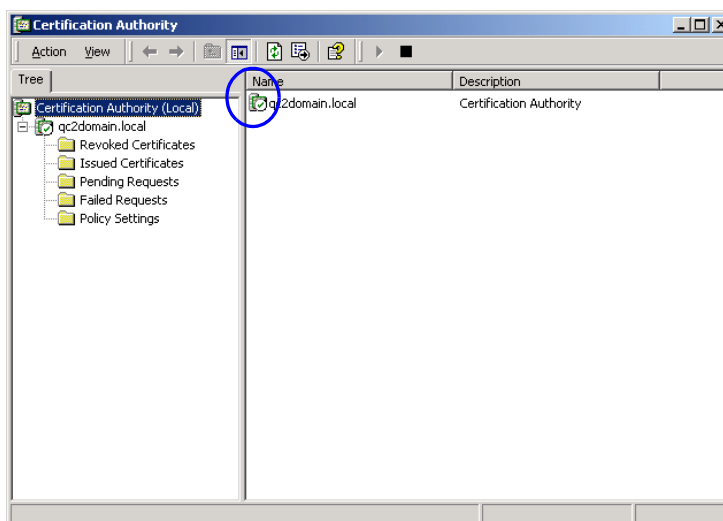


Fig. E-1 Certification Authority window

2. Verify that the certificate authority has been installed on this server and is up and running—indicated by a green check mark on the server icon (see circled item in Fig. E-1).

Locate Certificates folder

1. Go to Start > Run to open the Run dialog box. In the **Open** field, type in **mmc.exe** to specify that you wish to access the Microsoft Management Console:

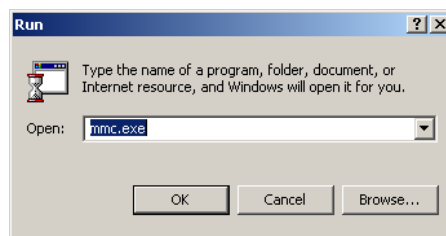


Fig. E-2 Run dialog box

2. Click **OK** to open the Console window:

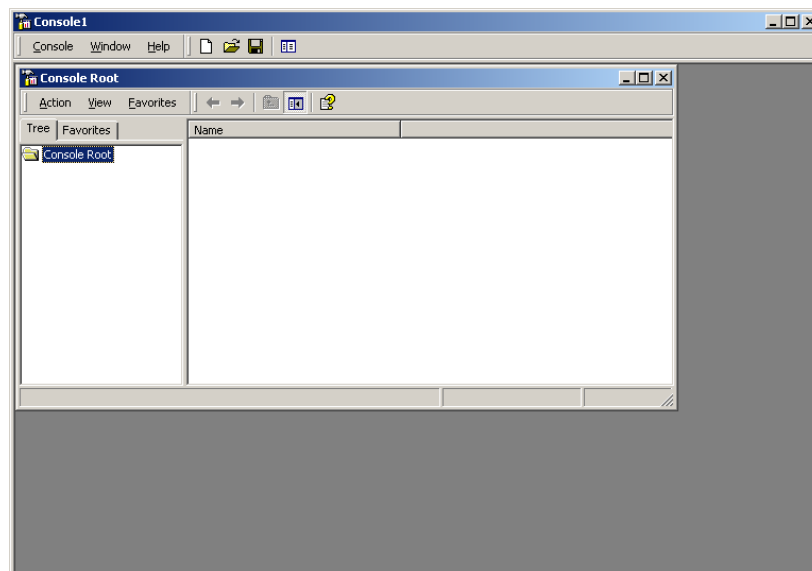


Fig. E-3 Microsoft Console window

3. From the toolbar, click Console to open the pop-up menu. Select Add/Remove Snap-in to open the Add/Remove Snap-in dialog box:

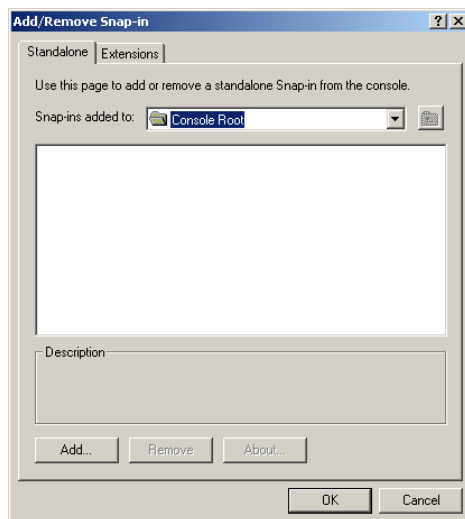


Fig. E-4 Add/Remove Snap-in

4. Click **Add** to open the Add Standalone Snap-in dialog box:

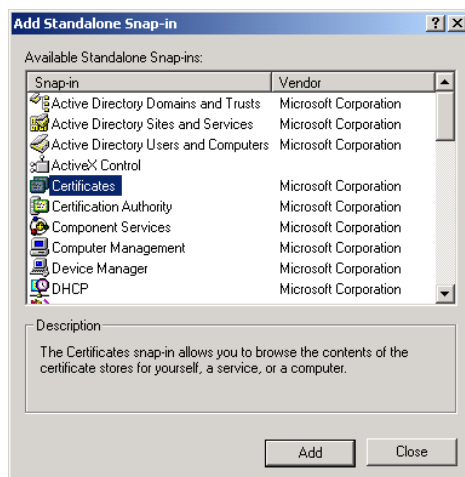


Fig. E-5 Add Standalone Snap-in

5. Select Certificates, and click **Add** to open the Certificates snap-in wizard dialog box:

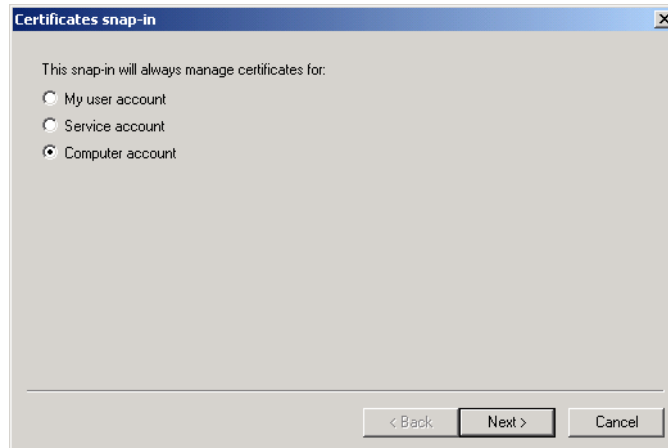


Fig. E-6 Certificates snap-in dialog box

6. Choose "Computer account", and click **Next** to go to the Select Computer wizard page:

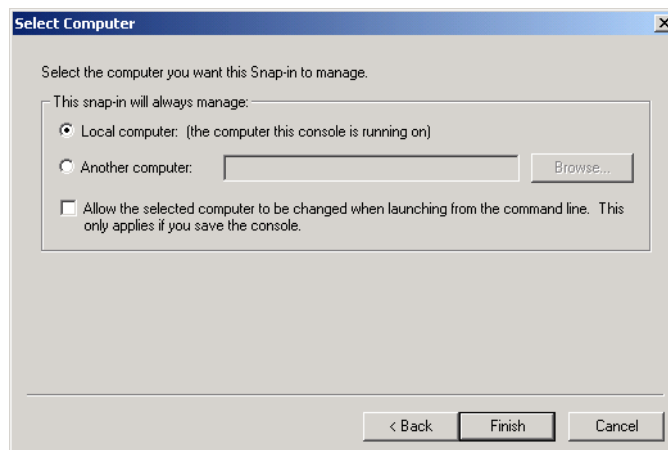


Fig. E-7 Select Computer dialog box

7. Choose "Local computer: (the computer this console is running on)", and click **Finish** to close the wizard dialog box.
8. Click **Close** to close the Add Standalone Snap-in dialog box. Click **OK** to close the Add/Remove Snap-in dialog box.

Notice that the snap-in has now been added to the Console Root folder:

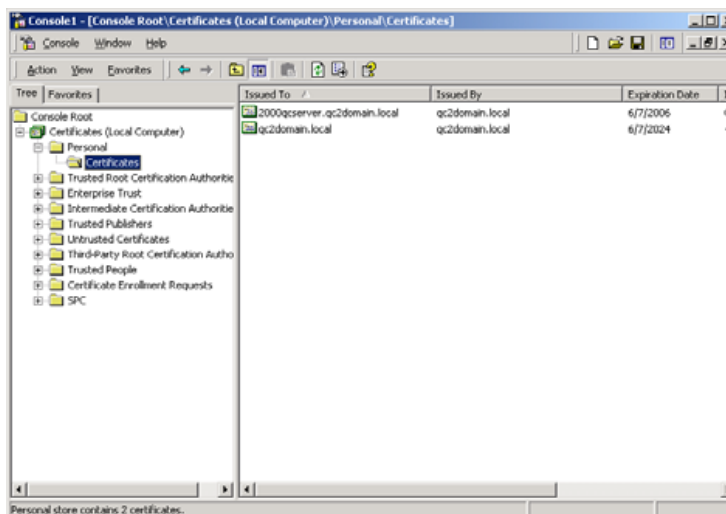


Fig. E-8 Console Root with snap-in

Export the master certificate for the domain

1. Go to the right panel of the Console and select the master certificate for the domain that you just added.
2. Right-click the certificate to open the pop-up menu, and select All Tasks > Export:

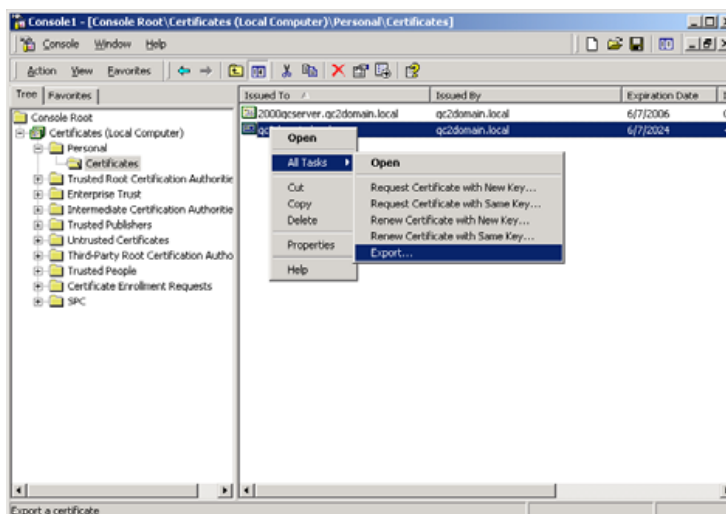


Fig. E-9 Select the certificate to be exported

This action launches the Certificate Export Wizard:



Fig. E-10 Certificate Export Wizard

3. Click **Next** to go to the Export Private Key page of the wizard:

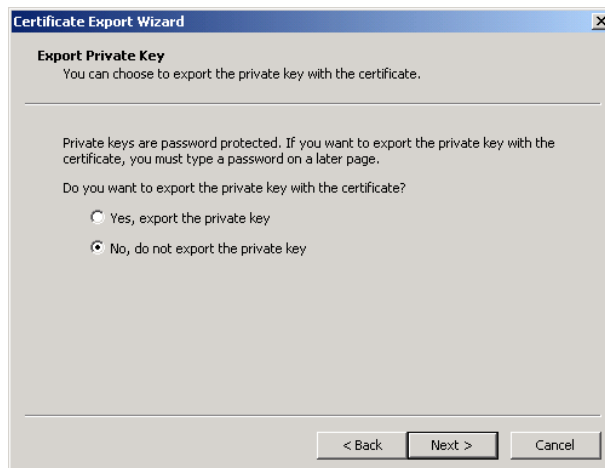


Fig. E-11 Export Private Key

4. Select “No, do not export the private key”, and click **Next** to go to the Export File Format page of the wizard:

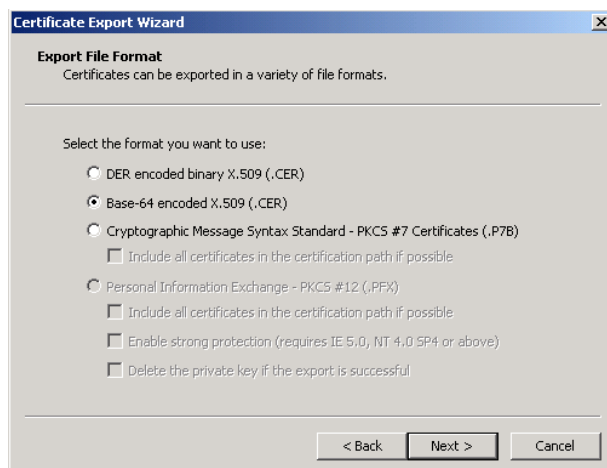


Fig. E-12 Export File Format

5. Select “Base-64 encoded X.509 (.CER)” and click **Next** to go to the File to Export page of the wizard:

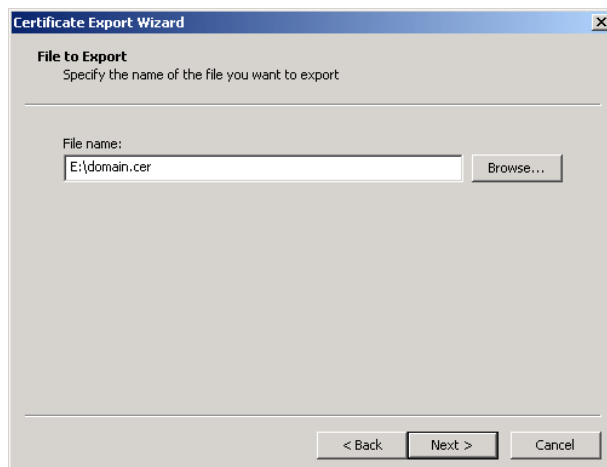


Fig. E-13 File to Export

6. Enter the **File name** of the file to be exported, followed by the **.cer** extension. Click **Next** to go to the final page of the wizard:



Fig. E-14 Settings

7. Notice that the specified settings display in the list box, indicating the certificate has been successfully copied from the console to your disk. Click **Finish** to close the wizard dialog box.
8. Close the Console.

The certificate can now be uploaded to the R3000.

Export a Novell SSL Certificate

1. From the console of the LDAP server, go to the tree in the left panel and open the Security folder to display the contents in the Console View (right panel):

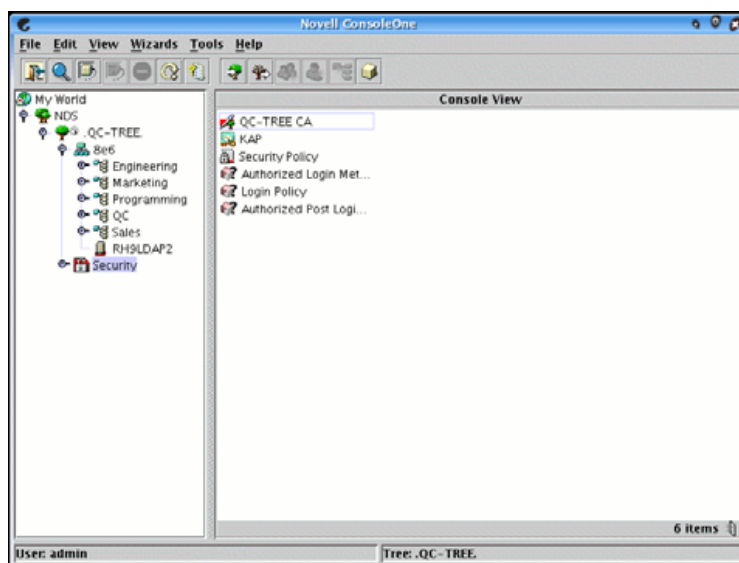


Fig. E-15 Novell Console window

2. Find the tree's folder and right-click it to open the pop-up menu. Select Properties to open the Properties dialog box:

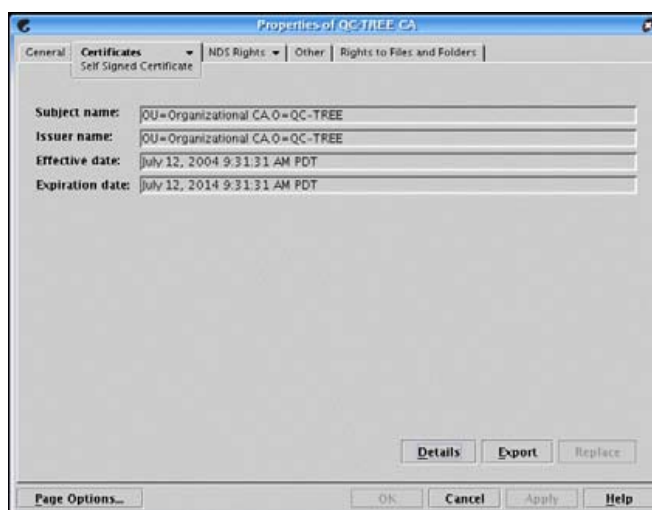


Fig. E-16 Properties dialog box

3. Click the Certificates tab to go to the Self Signed Certificate page.
4. Click **Export** to open the Export A Certificate pop-up window:

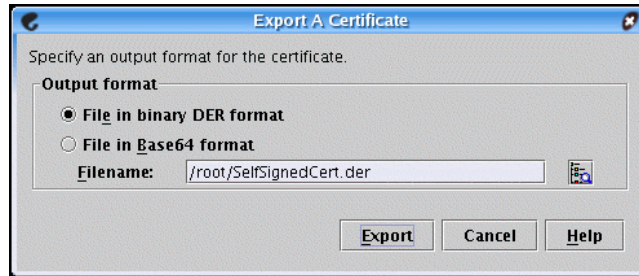


Fig. E-17 Export A Certificate pop-up window

5. Select “File in binary DER format” for the Output format. The path of the certificate displays in the Filename field.
6. Click **Export** to open another pop-up window that asks where you would like to save the certificate—the most convenient place would be your desktop.

The certificate can now be uploaded to the R3000.

Obtain a Sun ONE SSL Certificate

Unlike Microsoft or Novell, the Sun ONE LDAP directory does not have a tool for exporting an SSL certificate once it has been imported to the LDAP server.

Therefore, a copy of the root certificate—in the .cer or .der format—that was used to sign the LDAP server’s certificate must be uploaded to the R3000. This certificate can be an internally generated root certificate (if you have a certificate authority to generate the certificate), or can be the root certificate used by the external signing authority.

APPENDIX F

Override Pop-up Blockers

An override account user with pop-up blocking software installed on his/her workstation will need to temporarily disable pop-up blocking in order to authenticate him/herself via the Options page:

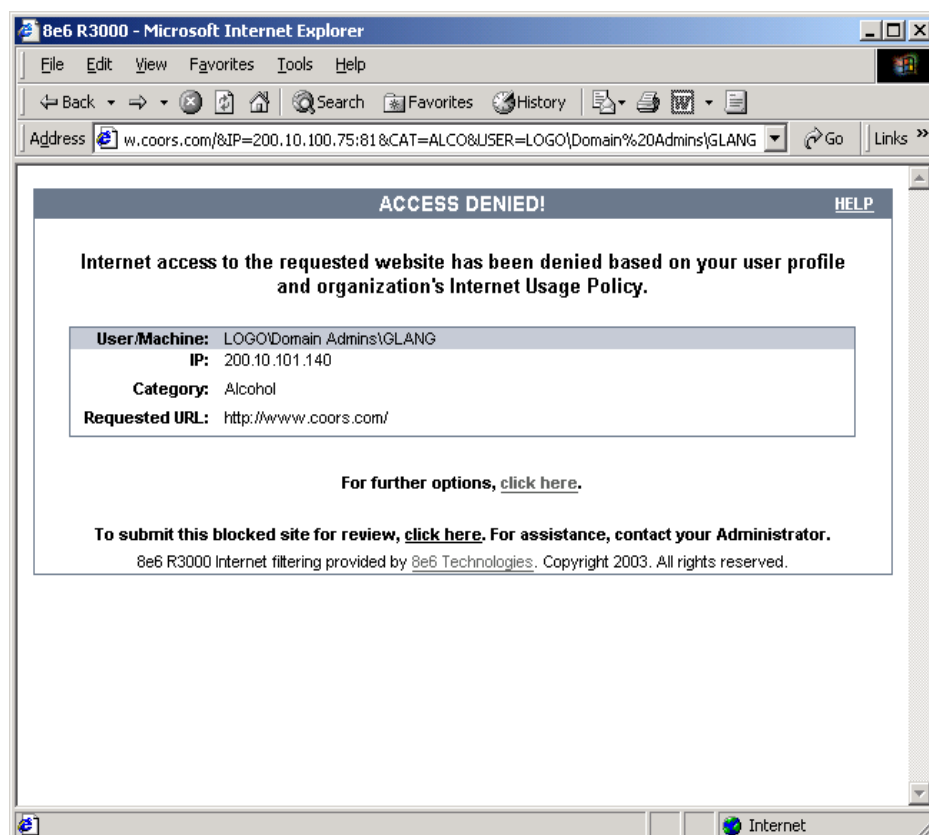


Fig. F-1 Options page

This appendix provides instructions on how to use an override account if typical pop-up blocking software is installed, as in the following products: Yahoo! Toolbar, Google Toolbar, AdwareSafe, Mozilla Firefox, and Windows XP Service Pack 2 (SP2).

Yahoo! Toolbar Pop-up Blocker

If pop-up blocking is enabled

1. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

Add override account to the white list

If the override account window was previously blocked by the Yahoo! Toolbar, it can be moved from the black list and added to the white list so that it will always be allowed to pass. To do this:

1. Go to the Yahoo! Toolbar and click the pop-up icon to open the pop-up menu:

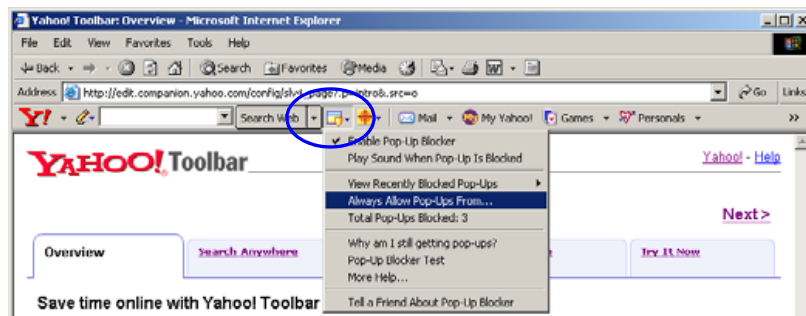


Fig. F-2 Select menu option Always Allow Pop-Ups From

2. Choose Always Allow Pop-Ups From to open the Yahoo! Pop-Up Blocker dialog box:

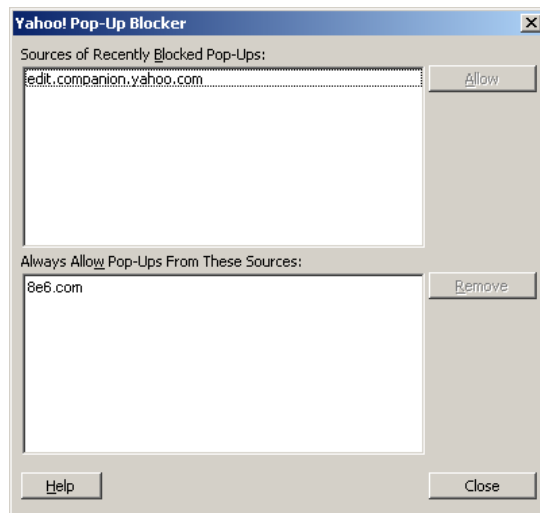


Fig. F-3 Allow pop-ups from source

3. Select the source from the Sources of Recently Blocked Pop-Ups list box to activate the Allow button.
4. Click **Allow** to move the selected source to the Always Allow Pop-Ups From These Sources list box.
5. Click **Close** to save your changes and to close the dialog box.

Google Toolbar Pop-up Blocker

If pop-up blocking is enabled

1. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

Add override account to the white list

To add the override account window to the white list so that it will always be allowed to pass, go to the Google Toolbar and click the # blocked icon:

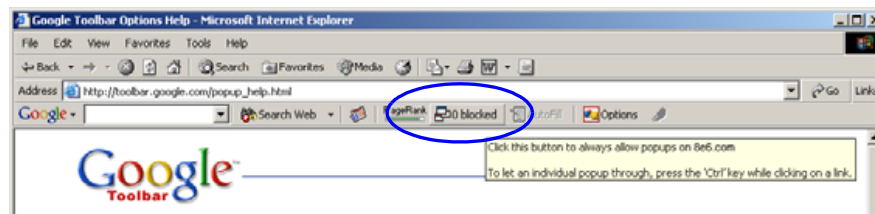


Fig. F-4 # blocked icon enabled

Clicking this icon toggles to the Site pop-ups allowed icon, adding the override account window to your white list:

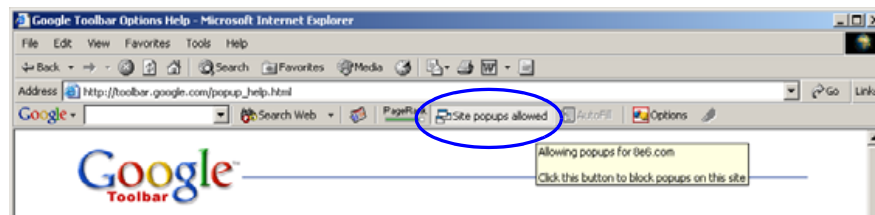


Fig. F-5 Site pop-ups allowed icon enabled

AdwareSafe Pop-up Blocker

If pop-up blocking is enabled

1. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

Temporarily disable pop-up blocking

AdwareSafe's SearchSafe toolbar lets you toggle between enabling pop-up blocking (# popups blocked) and disabling pop-up blocking (Popup protection off) by clicking the pop-up icon.

1. In the IE browser, go to the SearchSafe toolbar and click the icon for # popups blocked to toggle to Popup protection off. This action turns off pop-up blocking.
2. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
3. Click the **Override** button to open the override account pop-up window.
4. Go back to the SearchSafe toolbar and click the icon for Popup protection off to toggle back to # popups blocked. This action turns on pop-up blocking again.

Mozilla Firefox Pop-up Blocker

Add override account to the white list

1. From the browser, open the Preferences dialog box.
2. Go to the Category list box and select Privacy & Security > Popup Windows to display the Popup Windows page:

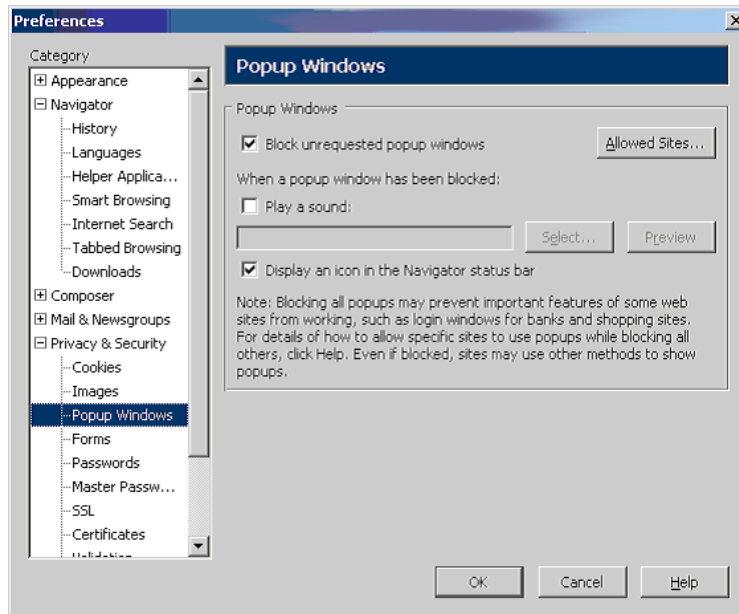


Fig. F-6 Mozilla Firefox Popup Windows Preferences

3. With the “Block unrequested popup windows” checkbox checked, click **Allowed Sites** and enter the URL to allow the override account window to pass.
4. Click **OK** to save your changes and to close the dialog box.

Windows XP SP2 Pop-up Blocker

Set up pop-up blocking

There are two ways to enable the pop-up blocking feature in the IE browser.

Use the Internet Options dialog box

1. From the IE browser, go to the toolbar and select Tools > Internet Options to open the Internet Options dialog box.
2. Click the Privacy tab:



Fig. F-7 Enable pop-up blocking

3. In the Pop-up Blocker frame, check “Block pop-ups”.
4. Click **Apply** and then click **OK** to close the dialog box.

Use the IE toolbar

In the IE browser, go to the toolbar and select Tools > Pop-up Blocker > Turn On Pop-up Blocker:

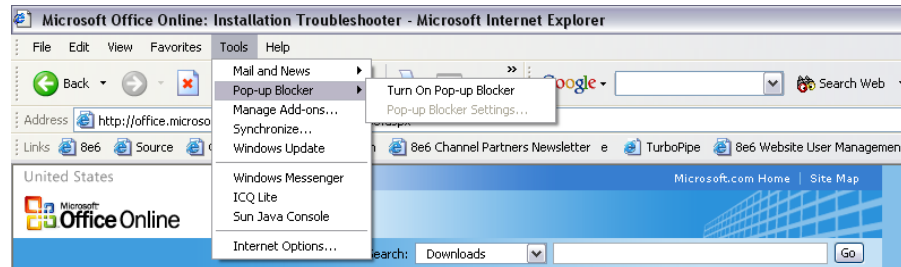


Fig. F-8 Toolbar setup

When you click Turn On Pop-up Blocker, this menu selection changes to Turn Off Pop-up Blocker and activates the Pop-up Blocker Settings menu item.

You can toggle between the On and Off settings to enable or disable pop-up blocking.

Temporarily disable pop-up blocking

1. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

Add override account to the white list

There are two ways to disable pop-up blocking for the override account and to add the override account to your white list.

Use the IE toolbar

1. With pop-up blocking enabled, go to the toolbar and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box:

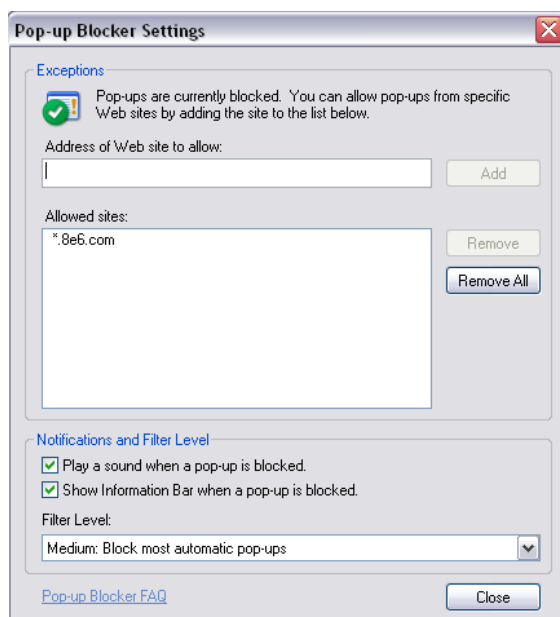


Fig. F-9 Pop-up Blocker Settings

2. Enter the **Address of Web site to allow**, and click **Add** to include this address in the Allowed sites list box. Click **Close** to close the dialog box. The override account window has now been added to your white list.
3. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
4. Click the **Override** button to open the override account pop-up window.

Use the Information Bar

With pop-up blocking enabled, the Information Bar can be set up and used for viewing information about blocked pop-ups or allowing pop-ups from a specified site.

Set up the Information Bar

1. Go to the toolbar and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box (see Fig. F-9).
2. In the Notifications and Filter Level frame, click the checkbox for “Show Information Bar when a pop-up is blocked.”
3. Click **Close** to close the dialog box.

Access your override account

1. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
2. Click the **Override** button. This action displays the following message in the Information Bar: “Pop-up blocked. To see this pop-up or additional options click here...”:

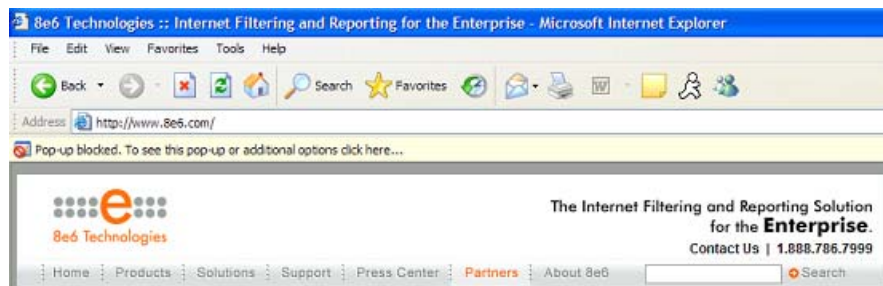
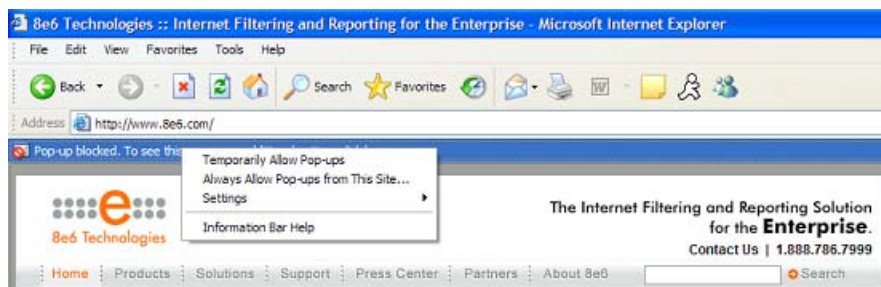
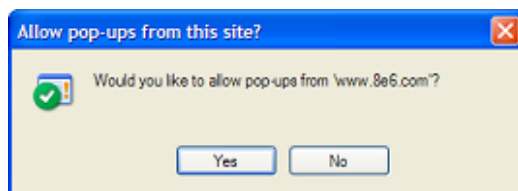


Fig. F-10 Information Bar showing blocked pop-up status

3. Click the Information Bar for settings options:

*Fig. F-11 Information Bar menu options*

4. Select Always Allow Pop-ups from This Site—this action opens the Allow pop-ups from this site? dialog box:

*Fig. F-12 Allow pop-ups dialog box*5. Click **Yes** to add the override account to your white list and to close the dialog box.

NOTE: To view your white list, go to the *Pop-up Blocker Settings* dialog box (see Fig. F-9) and see the entries in the *Allowed sites list box*.

6. Go back to the Options page and click **Override** to open the override account window.

APPENDIX G

Glossary

This glossary includes definitions for terminology used in this user guide.

ADS - Active Directory Services is a Windows 2000 directory service that acts as the central authority for network security, by letting the operating system validate a user's identity and control his or her access to network resources.

attribute - A component of a group base or Distinguished Name (DN) that has a type and value. Attribute types include "cn" for common name, "dc" for domain component, and "ou" for organizational unit.

authentication method - A way to validate users on a network. Methods include SMB/NT (referred to as "NT" throughout this user guide) and LDAP.

authentication server - The domain controller on a domain. This server is used for authenticating users on the network.

block setting - A setting assigned to a service port or library category when creating a rule, or when setting up a filtering profile or the minimum filtering level. If an item is given a block setting, users will be denied access to it.

common name (cn) - An attribute type entered for a username and group when using LDAP.

directory - This information source on a server contains attribute-based data relevant to a DN entry.

directory service - Uses a directory on a server to automate administrative tasks for storing and managing objects on a network (such as users, passwords, and network resources users can access). ADS, DNS, and NDS (Novell Directory Services) are types of directory services.

Distinguished Name (DN) - A string of “cn” and “dc” attribute types comprised of the username and group name, domain name, and DNS suffix. For example: “cn=admin_user, cn=admin, dc=yahoo, dc=com”. The “ou” attribute type also could be a part of the DN. For example: “cn=Joe Smith, ou=users, ou=sales, dc=acme, dc=com”.

DNS - Domain Name Service is a distributed Internet directory service. DNS is used mostly for making translations between domain names and IP addresses.

domain - An entity on a network comprised of servers, workstations, and peripherals.

domain component (dc) - An attribute type entered for a domain name and DNS suffix when using LDAP.

domain controller - An authentication server that answers logon requests from workstations in a Windows NT domain. There are two types of domain controller servers: Primary Domain Controller (PDC) and Backup Domain Controller (BDC).

entry - A collection of attribute types that comprise a Distinguished Name (DN). Each attribute type of the Distinguished Name has a type and one or more values. These types are mnemonic strings, such as “cn” for common name, “dc” for domain component, or “ou” for organizational unit.

filter setting - A setting made for a service port. A service port with a filter setting uses filter settings created for library categories (block or open settings) to determine whether users should be denied or allowed access to that port.

firewall mode - An R3000 set up in the firewall mode will filter all requests. If the request is appropriate, the original packet will pass unchanged. If the request is inappropriate, the original packet will be blocked from being routed through.

global administrator - An authorized administrator of the network who maintains all aspects of the R3000, except for managing master IP groups and their members, and their associated filtering profiles. The global administrator configures the R3000, sets up master IP groups, and performs routine maintenance on the server.

group administrator - An authorized administrator of the network who maintains a master IP group, setting up and managing members within that group. This administrator also adds and maintains customized library categories for the group.

group name - The name of a group set up for a domain on an NT server. For example: "production" or "sales".

invisible mode - An R3000 set up in the invisible mode will filter all connections on the Ethernet between client PCs and the Internet, without stopping each IP packet on the same Ethernet segment. The unit will only intercept a session if an inappropriate request was submitted by a client.

LDAP - One of two authentication method protocols used by the R3000. Lightweight Directory Access Protocol (LDAP) is a directory service protocol based on entries (Distinguished Names).

LDAP host - The LDAP domain name and DNS suffix. For example: "yahoo.com" or "server.local".

login (or logon) script - Consists of syntax that is used for re-authenticating a user if the network connection between the user's machine and the server is lost.

machine name - Pertains to the name of the user's workstation machine (computer).

minimum filtering level - A set of library categories and service ports defined at the global level to be blocked or opened. If the minimum filtering level is established, it is applied in conjunction with a user's filtering profile. If a user does not belong to a group, or the user's group does not have a filtering profile, the default (global) filtering profile is used, and the minimum filtering level does not apply to that user.

name resolution - A process that occurs when the R3000 attempts to resolve the IP address of the authentication server with the machine name of that server. This continuous and regulated automated procedure ensures the connection between the two servers is maintained.

net use - A command that is used for connecting a computer to—or disconnecting a computer from—a shared resource, or displaying information about computer connections. The command also controls persistent net connections.

NetBIOS - Network Basic Input Output System is an application programming interface (API) that augments the DOS BIOS by adding special functions to local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. NetBIOS relies on a message format called Server Message Block (SMB).

NetBIOS name lookup - An authentication method used for validating a client (machine) by its machine name.

Network Address Translation (NAT) - Allows a single real IP address to be used by multiple PCs or servers. This is accomplished via a creative translation of inside "fake" IP addresses into outside real IP addresses.

open setting - A setting assigned to a service port or library category when creating a rule, or when setting up a filtering profile or the minimum filtering level. If an item is given an open (pass) setting, users will have access to it.

organizational unit (ou) - An attribute type that can be entered in the LDAP Distinguished Name for a user group.

override account - An account created by the global group administrator or the group administrator to give an authorized user the ability to access Internet content blocked at the global level or the group level.

PDC - A Primary Domain Controller functions as the authentication server on a Windows NT domain. This server maintains the master copy of the directory database used for validating users.

profile string - The string of characters that define a filtering profile. A profile string can consist of the following components: category codes, service port numbers, and redirect URL.

protocol - A type of format for transmitting data between two devices. LDAP and SMB are types of authentication method protocols.

proxy server - An appliance or software that accesses the Internet for the user's client PC. When a client PC submits a request for a Web page, the proxy server accesses the page from the Internet and sends it to the client. A proxy server may be used for security reasons or in conjunction with caching for bandwidth and performance reasons.

router mode - An R3000 set up in the router mode will act as an Ethernet router, filtering IP packets as they pass from one card to another. While all original packets from client PCs are allowed to pass, if the R3000 determines that a request is inappropriate, a block page is returned to the client to replace the actual requested Web page or service.

rule - A filtering component comprised of library categories set up to be blocked or opened. Each rule created by the global administrator is assigned a number and a name that should be indicative of its theme. Rules are used when creating filtering profiles for entities on the network.

search engine - A program that searches Web pages for specified keywords and returns a list of the pages or services where the keywords were found.

service port - Service ports can be set up to blocked. Examples of these ports include File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Network News Transfer Protocol (NNTP), Secured HTTP Transmission (HTTPS), and Other ports such as Secure Shell (SSH).

SMB - One of two authentication method protocols used by the R3000. Server Message Block is a “client/server, request/response” protocol.

sub-group - An entity of a master IP group with an associated member IP address, and filtering profile.

time-based profile - A user profile used by both the NT and LDAP authentication methods to give a user a time limit on his/her Internet connection.

time profile - A customized filtering profile set up to be effective at a specified time period for designated users.

tiers - Levels of authentication methods. Tier 1 uses net use based authentication for NT or LDAP. Tier 2 uses time-based profiles for both the NT and LDAP authentication methods. Tier 3 uses persistent login connections for either the NT or LDAP authentication methods.

URL - An abbreviation for Uniform Resource Locator, the global address of Web pages and other resources on the Internet. A URL is comprised of two parts. The first part of the address specifies which protocol to use (such as "http"). The second part specifies the IP address or the domain name where the resource is located (such as "203.15.47.23" or "8e6.com").

virtual IP address - The IP address used for communicating with all users who log on the network.

Web-based - An authentication method that uses time-based profiles or persistent login connections.

white list - A list of approved library categories for a specified entity's filtering profile.

INDEX

Numerics

- 3-try login script 203
- 8e6 Authenticator 23, 42
- 8e6 supplied category 17

A

- Account tab 134
- Address tab 131
- ADS, definition 247
- alert box, terminology 3
- Alias List tab 137
- Alias Name 138
- always allowed 19
- Anonymous Bind 134, 143
- attribute, definition 247
- authentication
 - activate NT 203
 - activate on network 174
 - activate Web-based for Global Group 187
 - activated Web-based for IP group 175
 - configuration procedures 54
 - methods 27
 - net use based module diagram 25
 - net use based process 25
 - servlet 67
 - setup procedures 30
 - specifications and requirements 27
 - test net use settings 173
 - test settings 162
 - test Web-based settings 164
- Authentication Form Customization 93
- authentication method, definition 247
- Authentication Request Form 87, 162, 171
 - figure 162, 172
- authentication server 11
 - definition 247

- function in net use based process 25
- login scripts 32
- Authentication Settings window 70
 - join the domain 101
- authentication solution
 - single user compatibility chart 53
- Authentication SSL Certificate window 72
- authmodule.log 79

B

- Backup Domain Controller (BDC) 248
- backup server
 - Novell eDirectory 141
- Backup Server Configuration wizard 141
- Block page 83
- block page 13, 14
- Block Page Authentication 82
- Block Page Customization 97
- block setting 19
 - definition 247
- button, terminology 3

C

- category
 - custom categories 17
 - library 17
- category codes 211
- Category Profile
 - LDAP domain 158
 - NT domain 121
- Category tab
 - LDAP domain 158
 - NT domain 121
- checkbox, terminology 3
- Common Customization 90
- common name (cn), definition 247
- control panel, definition 3
- Create CSR 75
- Create Domain Controller 103

Create LDAP Domain dialog box 125
custom categories 17

D

Default Rule tab 139
dialog box, terminology 4
directory service, definition 248
directory, definition 247
Distinguished Name (DN)
 definition 248
 LDAP protocol 28
DNS, definition 248
domain
 definition 248
 delete profile 145
domain component (dc), definition 248
domain controller, definition 248
Domain Name Service (DNS) 248

E

edirAgent.log 79
eDirectory 23, 44, 50
 backup server 141
 Default Rule tab 141
edirEvent.log 79
Enable/Disable Authentication window 64
entry, definition 248
environment requirements 58
eth0, eth1 60, 63, 71

F

field, terminology 4
file formats 212
filter option codes 211
filter options 123, 160
filter setting 19
 definition 248
filtering 211
 category codes 211

- profile components 16
- profile types 12
- rules 20
- static profiles 13
- user, machine 14
- firewall mode 61, 62
 - definition 249
- frame, terminology 4
- FTP 59

G

- gateway IP address 62
- global administrator, definition 249
- global filtering profile 14
- global group 8
- grid, terminology 4
- group
 - global 8
 - IP 9
 - LDAP 11
 - NT 10
 - types of 8
- group administrator, definition 249
- group name, definition 249
- group objects 129
- Group tab 128
- Group/Member Details window
 - LDAP domain 155
 - NT domain 118

H

- HTTPS 59

I

- IANA 28
- individual IP member
 - profile type 13
- Internet Explorer 58
- invisible mode 61, 62

- definition 249
- IP group 9
 - diagram 9
- IPC share 25

J

- Java applet 68
- Java Plug-in 58
- Java Runtime Environment 58, 68
- Java Virtual Machine 58
- JavaScript 58
- join the domain 102

L

- LAN Settings window 62
- LDAP
 - Active Directory Service usage 35
 - authentication protocol 23
 - definition 249
 - domain diagram 11
 - domain groups 11
 - name resolution method 29
 - profile file format 153
 - protocol 28
 - server customizations 219
 - server setup 35
- LDAP domain
 - add 125
 - add groups, users 146
- LDAP domain window 126
- LDAP host, definition 249
- LDAP Query Base 133, 143
- LDAP Server Type 127
- LDAP User/Group Browser window 147
- library categories 17
 - category codes list 211
- list box, terminology 4
- lock profile 13
 - profile type 15

- log
 - view files 78
- login (or logon) script
 - definition 249
 - examples 32
 - usage 25

M

- machine name, definition 249
- Manually Add Group dialog box
 - LDAP 151
 - NT domain 114
- Manually Add Member dialog box
 - LDAP 150
 - NT domain 113
- master IP group 9
 - filtering profile 13
- methods
 - authentication 27
 - name resolution 29
- Microsoft Active Directory
 - Mixed Mode 30, 127
 - Native Mode 30, 127
- minimum filtering level 18
 - definition 250

N

- name resolution
 - definition 250
 - methods 29
 - WINS Server 29
- NAT
 - definition 250
- net use
 - command 203
 - definition 250
 - syntax 32
- NetBIOS
 - definition 250

- name lookup, definition 250
- NetBIOS Domain Name 132, 143
- NetBIOS name 70
- Netscape Directory Server 127
- Network Address Translation (NAT), definition 250
- network requirements 59
- NIC device 71
- Novell 23, 28, 30, 44, 48, 127, 136, 226
- Novell eDirectory Agent 50
- NT
 - domain diagram 10
 - domain groups 10
 - profile file format 116
- NT domain
 - add 103
 - Default Rule 107
 - Domain Settings 105
- NTLM authentication protocol 23, 101

O

- open setting 19
 - definition 250
- OpenLDAP 23, 147
 - server customizations 219
- Operation Mode window 60
- Options page 86
- organizational unit (ou), definition 251
- override account
 - AdwareSafe popup blocking 240
 - block page authentication 82
 - definition 251
 - Google Toolbar popup blocking 239
 - Mozilla Firefox popup blocking 241
 - override popup blockers 236
 - profile type 15
 - Windows XP SP2 popup blocking 242
 - Yahoo! Toolbar popup blocking 237

P

- PDC 102
 - definition 251
- pop-up blocking, disable 236
- pop-up box/window, terminology 5
- primary IP address 63
- Primary Domain Controller (PDC) 248
- profile string
 - definition 251
 - elements 210
- Profile window 120
 - LDAP domain 157
- protocol
 - definition 251
 - LDAP 28
 - SMB 27
- proxy server
 - definition 251
- pull-down menu, terminology 5

R

- radio button, terminology 5
- re-authentication
 - block page authentication 82
 - net use based process 26
- Redirect URL tab
 - LDAP domain 159
 - NT domain 122
- requirements
 - environment 58
- router mode 61, 62
 - definition 251
- rule 18
 - criteria 210
 - definition 251
- rules
 - LDAP server setup 35

S

- screen, terminology 5
- search engine, definition 252
- secondary IP address 63
- Select Groups/Members from Domain window 110
- Server Message Block (SMB), definition 252
- service port 18
 - definition 252
- session-based authentication (Tier 3) 23
- Set Group Priority window
 - LDAP domain 149
 - NT domain 111
- Single Sign-On
 - Novell eDirectory authentication 50
 - Tier 1 authentication 25
- single sign-on authentication (Tier 1) 23
- SMB
 - definition 252
 - disable Signing requirements in Windows 2003 221
 - protocol 27
 - Signing 27
- SMB/NT
 - name resolution method 29
- SSL certificate 73
 - Active Directory 226
 - Novell 234
 - obtain, export from LDAP server 226
 - Sun ONE 235
- SSL settings 135
- SSL tab 135
- SSO 50
- static filtering profiles 13
- sub-group
 - definition 252
- sub-topic
 - terminology 6
- Sun IPlanet 127
- Sun ONE 23
- Sun One 127
- system requirements 58

T

- technical support 206
- text box, terminology 6
- Tier 1
 - net use based authentication 25, 55, 66, 174
- Tier 1 and Tier 2 Script 39
- Tier 2
 - time-based, Web-based authentication 36
- Tier 2 Script 38
- Tier 2, Tier 3
 - Web-based authentication 55, 67, 174
- Tier 3
 - session-based, Web-based authentication 41
- tiers
 - definition 252
 - Web-based authentication 174
- time profile
 - definition 252
 - profile type 15
- time-based authentication (Tier 2) 23
- time-based profile 67, 82
- topic, terminology 6
- tree, terminology 7
- Type tab 126

U

- Upload User/Group Profile window
 - LDAP domain 152
 - NT domain 115
- URL, definition 252
- usage logs 78
- user objects 130
- User tab 130
- username formats 209

V

- View Log File window 78
- virtual IP address 32, 71
 - definition 252

W

- wbwatch.log 79
- Web-based authentication 54, 64, 72
 - block page authentication 82
 - SSL certificate 56
- Web-based, definition 253
- white list, definition 253
- window, terminology 7
- Windows 2003
 - SMB Signing 27
- WINS Server 70
 - name resolution usage 29
- workstation requirements 58